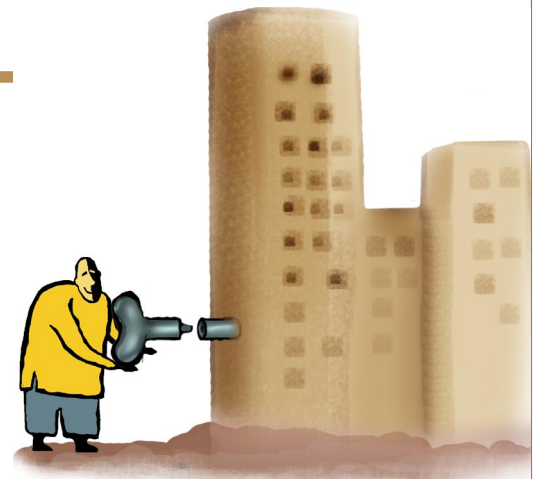


---

# UNDERSTANDING EVENT CORRELATION AND THE NEED FOR SECURITY INFORMATION MANAGEMENT

---



Enormous logs are produced by various network devices like IDS or Firewall, Webserver, applications and databases which is practically impossible to monitor manually. A single firewall alone can produce over 1 gigabyte of log data in a single day and IDS can produce over 500,000 messages over the same period. What's worse – much of the information generated by these security systems is dominated by false positives (an indication of hostile activity when there is none). The challenge is to isolate and prioritize the few messages that do indeed indicate real security threats. This need to isolate significant security incidents from the white noise of IDS, FW, OS, APPS, and AVS messages is part of the larger economic reality requiring organizations to utilize their existing security resources more effectively. Automation of the security operations workload and prioritization of tasks in the operations center is critical.

This white paper discusses how event correlation works and how a SIM (security information management) can fit into a corporate network to minimize the challenges faced by the system administrators or security professionals. Also, it discusses ways to reduce the time spend in analyzing huge logs produced by various network devices.

WHITE PAPER



DEBASIS MOHANTY

---



# Table of Contents

---

INTRODUCTION .....	3
TYPES OF EVENT CORRELATION .....	3
RULE-BASED .....	3
STATISTICAL BASED .....	3
SECURITY INFORMATION MANAGEMENT (SIM) .....	3
NEED FOR SIM .....	4
ADVANTAGE OF HAVING A SIM .....	4
WORKING OF A SIM .....	4
CHECKLIST FOR CHOOSING A SIM .....	7
CONCLUSION .....	9
ACRONYMS .....	9
REFERENCES .....	9
ACKNOWLEDGEMENTS .....	9
ABOUT THE AUTHOR .....	9
ABOUT WIPRO TECHNOLOGIES .....	10
WIPRO IN ENTERPRISE SECURITY SERVICES .....	10



## INTRODUCTION

The time it takes to read through and analyze the vast amount of transaction logs that can be produced will make security professionals spend too much time on unimportant events and not enough time responding to significant security threats. This process of addressing this issue is known as security information management and is the reason security event consolidation and correlation systems have become vital to the successful identification and handling of security incidents. Event consolidation brings together events from disparate systems into a central repository and event correlation monitors the various security events to determine which events are significant and which one relates to a particular attack.

## TYPES OF EVENT CORRELATION

There exists various kinds of correlation methods but here we discuss about two major approaches used for correlation by almost all SIMs. They are the rules-based and the statistical-based approaches.

### Rule-based

Rule-based correlation engine has some pre-existing knowledge of the attack (the rule) and from this, it is possible to define what has actually been detected in precise terms. Such attack knowledge is used to relate events and analyze them together in a common context.

These patterns can be pre-defined rules provided by vendors or they can be developed by the systems administrator over time. For example, an administrator could define a rule that would monitor port scans on their network devices. If it is found that these port scans are trying to identify open telnet ports, the rule could then monitor for telnet connection attempts during a predefined period after the port scans. If a telnet connection is identified and has originated from an unknown IP address, the event correlation system would send an alert to the management console or alternatively to a pager, email address or cell phone.

### Statistical-based

This kind of correlation does not employ any pre-existing knowledge of the malicious activity, but instead relies upon the knowledge (and recognition) of normal activities, which has been accumulated over time. Ongoing events are then rated by a built-in algorithm and may also be compared to the accumulated activity patterns, to distinguish normal from abnormal (suspicious).

These types of systems analyze events over a period of time and use weighted values to rate assets, systems and attackers. These weighted values are then analyzed to determine the risk of this type of attack occurring. These systems also set baseline levels of normal network activity and look for deviations from these normal behavior patterns that may indicate an attack.

## SECURITY INFORMATION MANAGEMENT (SIM)

SIM is a solution which allows automated integration of log analysis, event correlation, and reporting of critical security event information to enable organizations to immediately identify and respond to various threats.



## Need for SIM

The best way to increase the effectiveness of information security architecture for an organization is through better analysis and an increasingly popular analysis technique is event correlation. Unfortunately, conducting correlation without using security event management software is nearly impossible because of the following issues:

- Event data is logged in a variety of proprietary formats making comparison difficult.
- Event data is stored in multiple information 'silos', i.e. proprietary consoles, syslogs etc.
- Manually comparing event data from across the enterprise to find similarities is time consuming, if not impossible.
- No manual method exists that enables correlation to be conducted in real time.
- Constantly evolving threats necessitates continuously adding, modifying and enhancing correlation techniques.

## Advantages of Having an SIM

The advantages of having a SIM in a corporate network are as follows:

- Reduces overheads of network security professionals
- Reduces response time to identify real threats and take actions
- Reduces the number of false positives collected from the logs of various security devices
- Fine Tuning of the logs from different devices (servers, FW, AV or routers etc.) into one single format
- Helps in monitoring security logs of whole network at one single terminal

## Working of a SIM

There are four major components of a SIM. They are client components, correlation engine, signature database and a management console.

Most of the SIM are designed to be implemented in three tier architecture. The client component is installed on the systems or devices for which events has to be monitored. These client components then collect various event logs from the systems or devices and pass it to the correlation engine. The correlation engine then further analysis and validate the event logs sent by the client components based on rules or statistics stored in the database. Once the event is validated then it is passed on to the management console where the security professionals can view the alerts in one single console. The security professionals can view and monitor events related to various devices or servers in one single format and in one single console. Figure 1 which gives a clear picture of a standard architecture of a SIM.

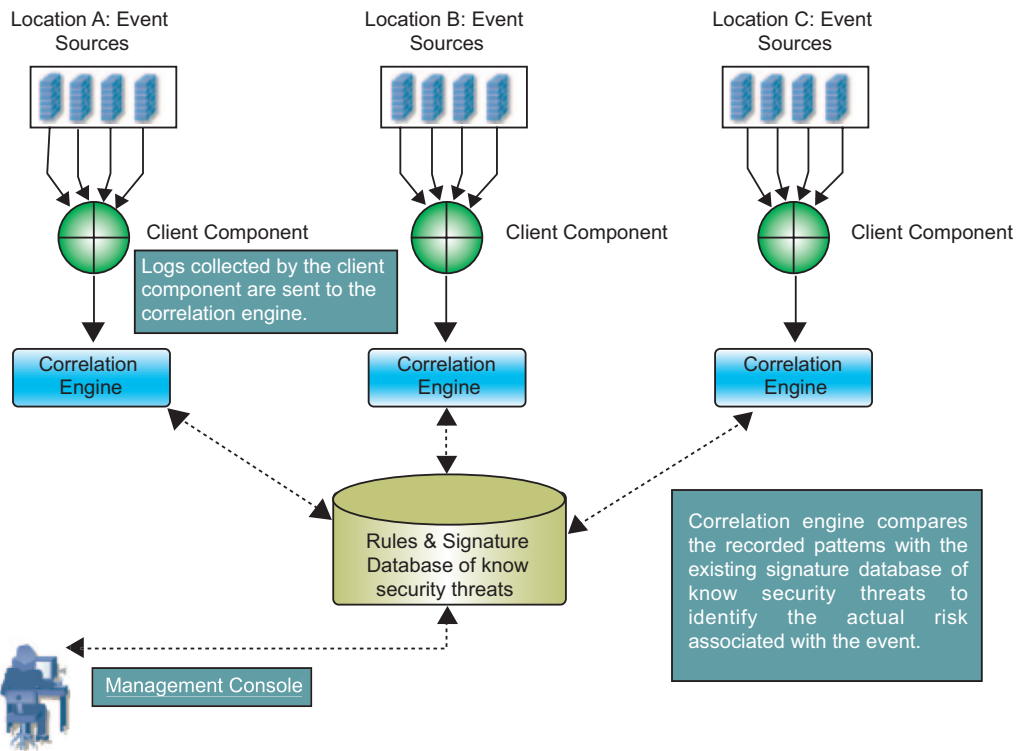


Figure 1: Screenshot showing the working of an SIM

Here we shall take one case study as a proof of concept (POC) to demonstrate how a correlation engine analyze and correlate events of an IIS Unicode attack on a Webserver. Figure 2 shows simulation of an IIS Unicode attack where an attacker is trying to exploit the IIS Webserver for its Unicode vulnerability. Exploiting this vulnerability an attacker can get access to the remote "cmd.exe" on the remote windows server and can execute commands of his/her choice.

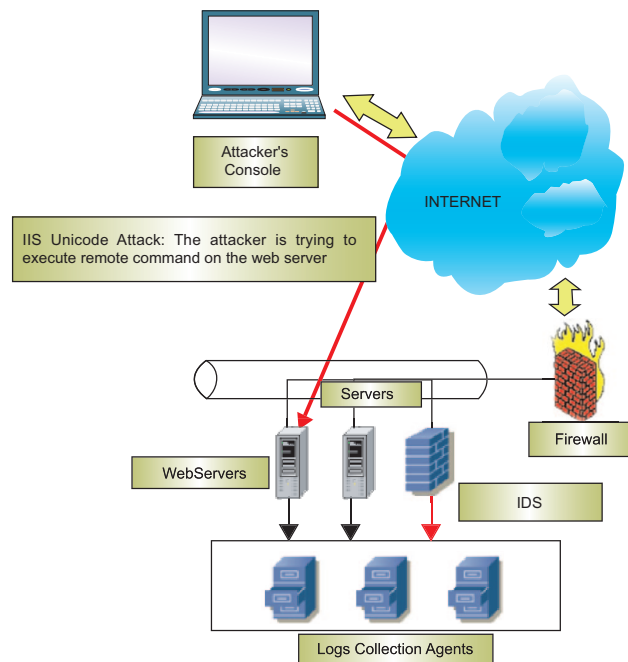


Figure 2: Screenshot showing IIS Unicode attack



When an attacker scans for IIS Unicode vulnerability or tries to exploit that vulnerability then these are detected by IDS and then the client components for IDS will send the events to the correlation engine for further analysis and validation of event.

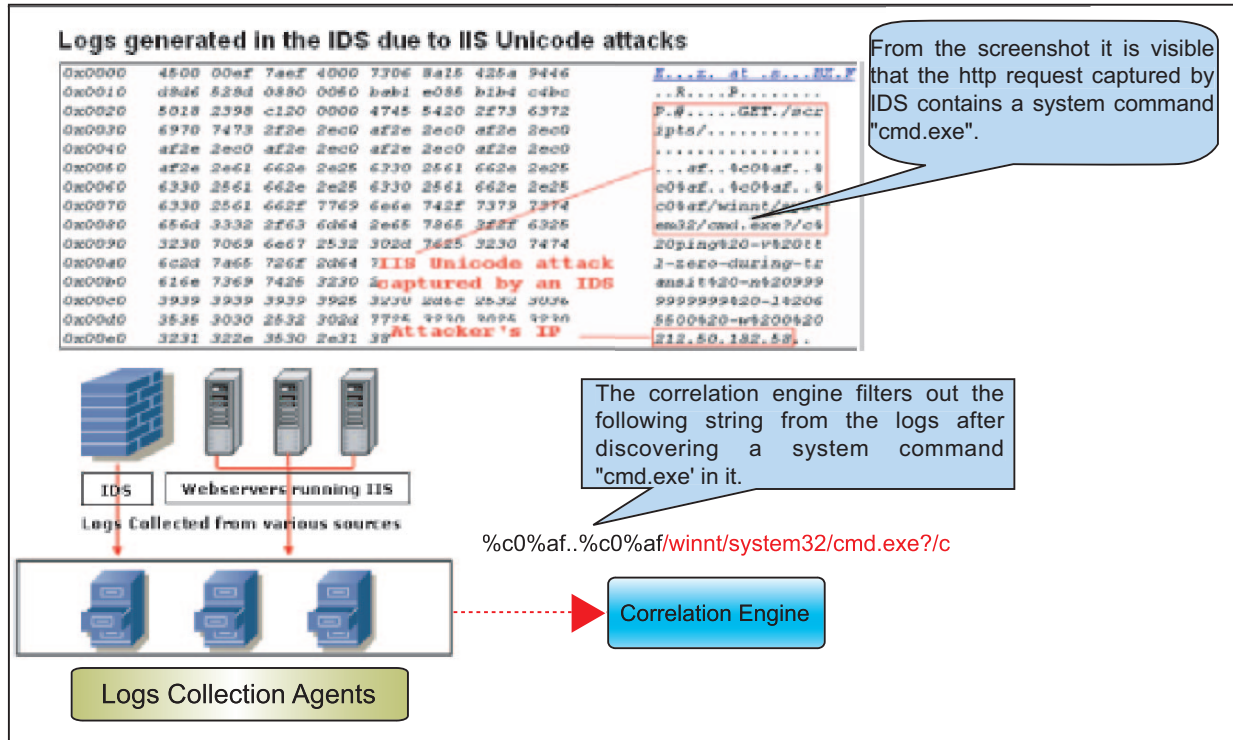


Figure 3: Screenshot showing IDS Logs displaying IIS Unicode attack

Once the correlation engine receives any events from the client components then it tries to analyze or correlate the events based on rules or statistics.

### Rules- based System

In this case the security threats are defined in the correlation database itself. Here a logical analysis is done by the correlation engine before drawing any conclusion.

Here, in this case (refer Figure 4) patterns of known security threats are compared with the pre-defined rules or the rules created by the SIM administrators.

In case of IIS Unicode attack, the analysis is done in the following manner:

Condition A: Logs from IDS, containing malicious web requests which contain system commands 'cmd.exe'.

Condition B: Logs from IDS, containing malicious web requests which contain system commands 'cmd.exe'.

Rule No #01IISUNI: Contains patterns of known IIS Unicode based attacks.

The correlation engine validates each condition by cross checking the conditions with each other and then tries to match with any predefined rules in the rules database. Once the rule is matched with any condition, then it raises an alert.

Here since 'Condition A' and 'Condition B' both validated that there was a malicious web requests which contain system commands 'cmd.exe', it was then validated with the 'Rule No #01IISUNI'. Once the rule confirms the attack as IIS Unicode, then an alert is raised at the management console.

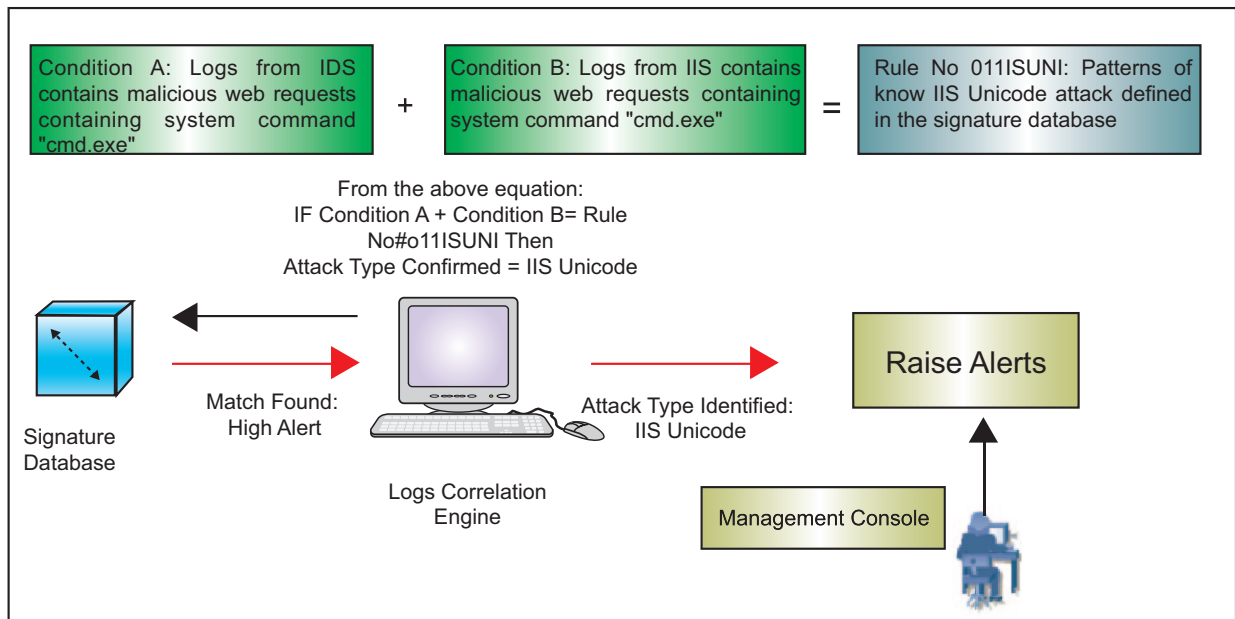


Figure 4: Screenshot showing the working of a rules-based correlation

### Statistical-based system

Statistical analysis is a time and weight based analysis. In this type of analysis, corporate companies have to rank their IT assets (servers and network devices etc.) in terms of value to the company or potential loss of value if the system is compromised.

Most the popular event correlation engine follows the following rule while determining the risks of an attack for a particular asset:

$$\text{Risk} = \text{Asset (value)} \times \text{Vulnerability (severity)} \times \text{Threat (criticality)}$$

Here, in case of IIS Unicode attack (refer Figure 3), if the Webserver is compromised and the server has been categorized as a critical asset by the corporate, then the risk factor is 'critical'. The greater the 'criticality' or the 'severity' or 'asset value', the greater is the risk factor.

## CHECKLIST FOR CHOOSING AN SIM

With the growing competition among SIM product vendors, there is always confusion in choosing the right kind of SIM product for any organization. All the SIM vendors will try to portray their product in different manners displaying same technology with different jargons to confuse the customers. To reduce such confusion, we have listed out a basic checklist based on which any organization can choose any SIM product easily.



Below given is a basic checklist for choosing the right SIM for an organization:

**Events and logs archiving**

- Centralized logs archival and storage
- Data integrity during transfer
- Real-time monitoring

**Events and logs analysis**

- Alerts suppression
- Event correlation logic and performance
- Audit logs data repository for forensic analysis
- Flexible filtering, actions and alerts

**Architecture**

- Centralized vulnerability database
- Centralized policy management
- Remote or Web-based management
- Cross-platform event management
- Multi-user support
- Access control based on user's roles

**Scalability**

- Multiple data base (Oracle, MS SQL etc.) support
- Extended platform (Windows, Linux, Solaris etc) coverage
- Network products (routers, firewalls, IDS etc.) support
- Support for active-directory environment

**Summary and reporting**

- GUI tools for collecting and viewing reports
- Secure Web-based tool for intelligence and reporting
- Variety of reporting format support (PDF, DOC, TXT etc.)
- Customizable reports
- Integration with online helpdesk with interactive trouble ticketing.

**Service and support**

- State-of-the-art technology
- Multiple, fully operational, fully redundant customer support located worldwide



## CONCLUSION

SIM technology continues to lead the way toward integration with variety of products and accepting input from virtually any networked product and combining that input with a wide array of analytical functions. Security threats are increasing in both frequency and complexity. Therefore, any security event correlation must increase in functionality. This results in effective security monitoring from both internal and external threats. The bottom line is that any organization will be able to respond to critical threats in real time.

## ACRONYMS

## REFERENCES

1. [http://www.giac.org/practical/GSEC/Kevin\\_McIntyre\\_GSEC.pdf](http://www.giac.org/practical/GSEC/Kevin_McIntyre_GSEC.pdf)
2. [http://www.netforensics.com/download/nF\\_Comprehensive\\_Correlation.pdf](http://www.netforensics.com/download/nF_Comprehensive_Correlation.pdf)

## ACKNOWLEDGEMENTS

The author would like to thank Mr. Srikanth Geddada (Practice Head, Managed Security Services) for his support and encouragement in writing this paper.

## ABOUT THE AUTHOR

Debasis Mohanty is currently working as a Team Lead for Penetration Testing at Managed Security Services of Wipro Technologies. Penetration testing, vulnerability research, reverse engineering, virus & worms analysis and cyber-crime investigations are some of his core expertise areas. Debasis is a member of various vulnerability research groups and his findings can be spotted on various Websites like SecurityFocus, ISS X-Force, Secunia, OSVDB etc. Debasis is also the author of several articles on penetration testing & malicious code research and is credited with a number of awards. He is also accredited by organizations like BlackHat-US, CSI (India), ISECOM.ORG and Application Security, Inc.



## ABOUT WIPRO TECHNOLOGIES

Wipro is the first PCMM Level 5 and SEI CMMi Level 5 certified IT Services Company globally. Wipro provides comprehensive IT solutions and services (including systems integration, IS outsourcing, package implementation, software application development and maintenance) and Research & Development services (hardware and software design, development and implementation) to corporations globally.

Wipro's unique value proposition is further delivered through our pioneering Offshore Outsourcing Model and stringent Quality Processes of SEI and Six Sigma.

## WIPRO IN ENTERPRISE SECURITY SERVICES

Wipro Enterprise Security Services (ESS) is a fast growing team in Wipro, which has been helping customers on the broad spectrum of information security needs for more than five years. With over 250 certified consultants and more than 100 successful projects to its credit, ESS is a highly skilled group capable of catering to various customer needs across the entire spectrum of businesses and industries.

For further information visit us at: <http://www.wipro.com/services>

For more whitepapers logon to: <http://www.wipro.com/insights>

© Copyright 2005. Wipro Technologies. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Wipro Technologies. Specifications subject to change without notice. All other trademarks mentioned herein are the property of their respective owners. Specifications subject to change without notice.

### Worldwide HQ

Wipro Technologies,  
Sarjapur Road,  
Bangalore-560 035,  
India.

### U.S.A.

Wipro Technologies  
1300 Crittenden Lane,  
Mountain View, CA 94043.

### U.K.

Wipro Technologies  
137 Euston Road,  
London, NW1 2 AA.

### France

Wipro Technologies  
91 Rue Du Faubourg,  
Saint Honoré, 75008 Paris.

### Germany

Wipro Technologies  
Horn Campus,  
Kaistrasses 101,  
Kiel 24114.

### Japan

Wipro Technologies  
# 911A, Landmark Tower,  
2-1-1 Minatomirai 2-chome,  
Nishi-ku, Yokohama 220 8109.

### U.A.E.

Wipro Limited  
Office No. 124,  
Building 1, First Floor,  
Dubai Internet City,  
P.O. Box 500119, Dubai.

[www.wipro.com](http://www.wipro.com)

eMail: [info@wipro.com](mailto:info@wipro.com)