WHITE PAPER

CISCO IPS SENSOR-LEVEL EVENT CORRELATION USING META EVENT GENERATOR (MEG)

Security administrators of traditional intrusion detection and prevention systems (IDSs/IPSs) have had difficulty effectively classifying the fidelity of IDS alarms received at the monitoring console. The accuracy of such classifications is dependent on several functions, including the sophistication of signature encoding, advanced risk-balanced rating algorithms, and target-based attack relevancy ratings. However, event correlation plays an important role in giving users information that is critical for arriving at informed decisions on how to mitigate today's sophisticated worms and viruses.

Cisco® IPS Sensor Software Version 5.0 incorporates advanced sensor-level event correlation that gives security administrators an automated method for enhancing the confidence level of the classification of malicious activity detected by the sensor. This provides a mechanism that allows for corresponding actions to deliver networkwide containment of worm and virus injection vectors, as well as worm propagation. This is accomplished through the following techniques:

- Correlation of alarms pertaining to worms that exploit multiple vulnerabilities
- Meta event generation for sequences of actions leading up to worm infestation
- Automated elevation of severity ratings when groups of events signify worm/virus activity
- Enhancement of alarm fidelity through simultaneous triggers based on hybrid detection algorithms

Each of these techniques is covered in the following paragraphs.

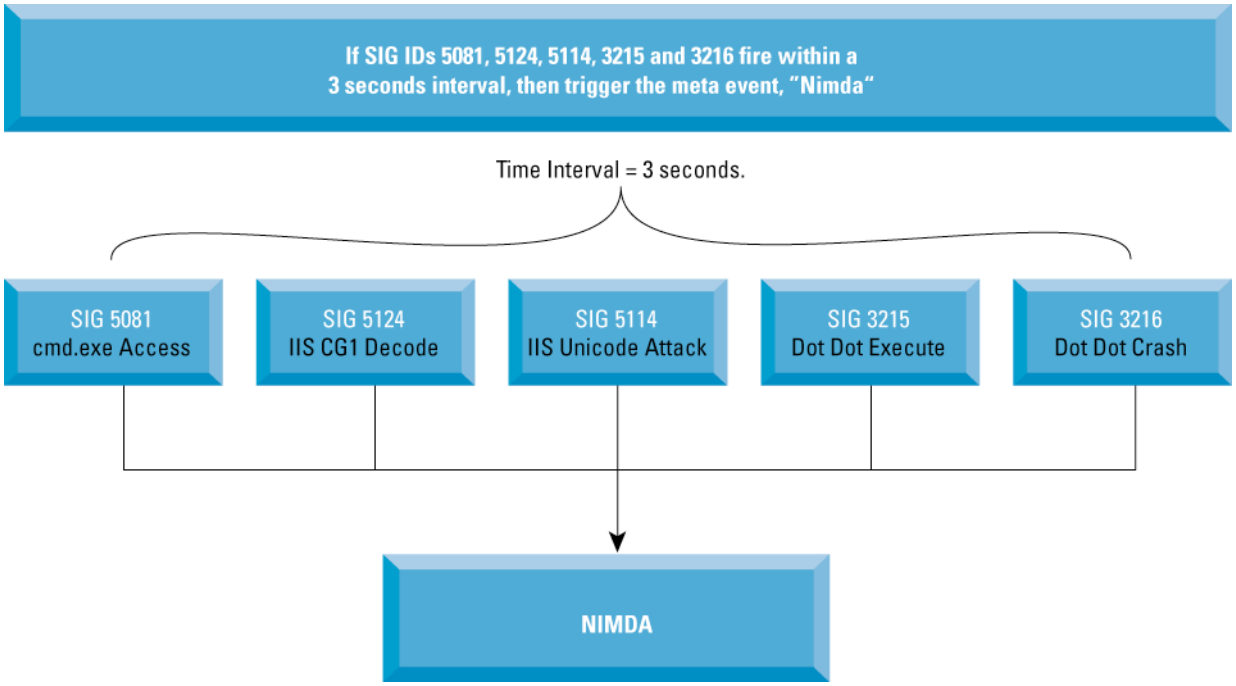
Nimda is a prime example of a worm that exploited multiple vulnerabilities during its propagation across networks. Typically, the various alarms that pertain to each of these exploits will trigger within a short time interval. The Meta Event Generator (MEG), delivered by Cisco IPS Sensor Software Version 5.0, takes the guesswork out of making an accurate assessment on the occurrence of multifaceted worms, such as Nimda. Using MEG, the user can specify logic that will consolidate all events pertaining to a certain worm into a single meta event, called "Nimda", for example (Figure 1). In doing so, the user can also specify a time interval during which these disparate events must be detected in order for the correlation algorithm to trigger the actual meta event.

Through the use of similar logical parameters, MEG can also be customized to deliver protection from environment-specific threats that may not be related to a universally known worm activity.

Lastly, knowing that the security knowledge base within organizations may not be sufficient to formulate the underlying logical algorithm on which a particular meta event is based, signature updates delivered by Cisco Systems that pertain to multifaceted worms such as Nimda will also deliver the associated meta event. Along with this meta event, the user will be given information that indicates the individual signatures that form the meta event.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 1. Event Correlation of Alarms Pertaining to Worms that Exploit Multiple Vulnerabilities, Using Nimda as an Example

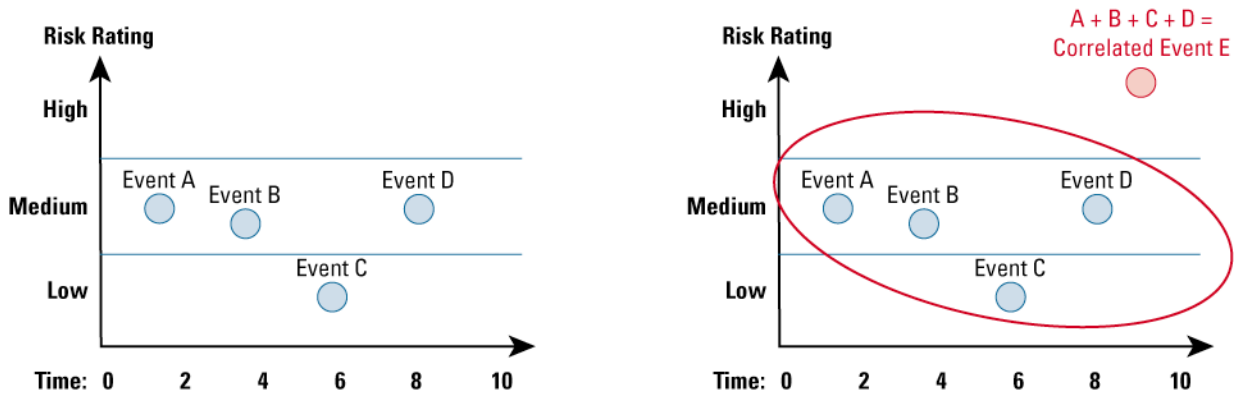


Historical trend analyses performed to characterize the lifecycle of worms often reveal a certain sequence of actions that are detected just prior to penetration. These actions occur in the "probing phase", when a chain of reconnaissance activities is performed against the target network. MEG allows the user to define the precursors to worm penetration by specifying a logical algorithm that triggers when a particular sequence of events occur. For example, if a certain number of hosts are pinged, followed by port scans on a defined set of ports, followed by a buffer overflow targeting hosts on a particular range of IP addresses, then trigger a single meta event "X". In this case, the resulting meta event will attain a higher fidelity rating by virtue of the correlation that was performed. Additionally, this meta event can be assigned an automated response action that will stop the worm that has been detected.

As worms propagate through the network, they typically generate multiple IPS events of varying degrees of severity. When there is no relationship established between such disparate events they could be assigned low severity ratings since, by themselves, they do not pose a significant threat. However, when these events are considered in the context of a sequence of related events, they could collectively indicate worm or virus activity. Cisco's Meta-Event Generator links these seemingly unrelated lower severity alarms into a high severity, high risk event, enabling the user to confidently drop the associated packets (see Figure 2).

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Figure 2. Meta Event Generator to correlate multiple events at low severity levels to a single worm event at a high severity level. Inline IPS drop actions can be reliably assigned to the correlated event to stop the worm or virus activity.



Lastly, MEG can be used to correlate events that are generated through the use of the hybrid detection techniques available in Cisco IPS Sensor Software. For example, if a denial of service (DoS) activity is detected through the triggering of a traffic anomaly algorithm and a classical “flood” type of signature, MEG can be used to corroborate one event with the other, thereby delivering a single meta event that indicates a higher likelihood that the DoS activity has actually occurred. As always, the most appropriate response actions could then be configured to mitigate the DoS condition.

In summary, MEG delivers an extensible architecture that provides sensor-level event correlation and corroboration, taking the guesswork out of event management and giving the user the enhanced capability of making intelligent decisions for the mitigation of malicious activities that relate to such events. The effectiveness of IPSs is greatly enhanced when such correlation algorithms are embedded into the sensor, as opposed to performing such methods at the monitoring console. When event correlation isd performed at the sensor level, the sensor can proactively take automated response actions that can effectively stop worms and viruses.

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)

204107_ETMG_MH_11.04

Printed in the USA

© 2004 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com