Global Information Assurance Certification Paper

Security Tools Review – The Security Dashboard

GIAC GSEC Practical v1.4

Peter C. Reverman

Revision 1.1

October 17, 2002

Table of Contents

Terminology

Definitions, Acronyms, and Abbreviations

IA:	Intrusion Analyst
IT:	Information Technology
SIM:	Security Information Manager
HIDS:	Host Intrusion Detection System
NIDS:	Network Intrusion Detection System
DIDS:	Distributed Intrusion Detection System
HIPS:	Host Intrusion Prevention System
NIPS:	Network Intrusion Prevention System
ACL's:	Access Control Lists
MSSP:	Managed Security Service Provider
DoS:	Denial of Service

Abstract

The “Security Dashboard” is a collection of security software tools that could be used to help solve the information overload problem created by too many security detection devices and dashboards. These tools provide central monitoring, reporting, reduction of false positives through event correlation, advanced filtering languages to isolate specific events, visualization of data, and increase confidence that the attack alerts are valid attacks and not false positives. Central security dashboard software products or SIM (Security Information Manager) products were reviewed for functionality that exists today. Some of the functionality includes the ability to centralize the monitoring function and reduce the number of sensor dashboards to monitor, filter data with event correlation, and manage cases for investigation. They provide summarization of alert data and data mining tools can be used for various purposes. Using a normalized database the alerts can be ranked by severity and prioritized for investigation. Visualization tools were also reviewed as another way to analyze the event data as they provide the ability to utilize the high sensing bandwidth of human sight to analyze network and host data that may help find or prevent attacks.

This document lists some of the tools available that are used to effectively monitor and investigate alerts provided by multiple heterogeneous security sensors such as HIDS, NIDS, Syslog data from routers, and firewall logs. The business requirements of managing a security information service drive the need to review the tools. The common business problem these tools attempt to solve is information overload of sensor data reducing the ability to detect attacks. This overload causes a resource drain on enterprise IT staff and may eliminate the protective value of the security tools deployed in an enterprise. HIDS and NIDS sensors can produce millions of “events” that may require large amounts of time to filter out false positives. In a constantly changing environment a human decision maker is always required to determine “good” packets from “bad” packets because new applications create new alerts requiring ongoing signature tuning.

The deployment of multiple security tools create multiple sources of data which are very time consuming to review independently and resources are typically not available to effectively monitor, tune, and maintain these tools in enterprise IT budgets. Many firms will outsource the monitoring function to an MSSP (Managed Security Service Provider) to cost effectively perform this function of aggregating security sensor real-time alerts and filtering them with correlation logic to reduce false positives. This document outlines some of the business requirements of security analysis but definitely not all requirements. The scope of this document covers the high-level requirements for security analysis and some possible requirements for a robust centralized event management function.

The Problem Statement

A large amount of inbound data will result from the deployment of host intrusion detection software, network intrusion detection sensors, firewalls, routers, switches, and other sources of network and application data. This data will need to be analyzed in real-time to provide an attack identification and mitigation by a group of security analysts protecting an enterprise from attack. To reduce the time of removing false positive information and find actual anomaly data tools will be required to filter the alerts so analysts can find and identify attacks more quickly and provide a better ROI. This attack information will lead to application profiling and system quarantine and cleanup and patch deployment to mitigate these attacks. The "Security Dashboard" is a collection of tools to solve the problem of large amounts of data received from the alerts and provide a quick identification and mitigation service.

System Purpose

The security dashboard is a set of tools used by security analyst groups within an enterprise to provide efficient information centralization, attack investigation, intrusion analysis, case management, visualization of network traffic, in-depth understanding of application behavior, and other identifiable characteristics of computer systems application and network behavior. The ability to identify actual attacks more quickly and avoid false positives is some of the value of these tools as well as visual depictions of network and application events for quicker analysis. Additional tools for "Active Listening" or maintaining an understanding of current vulnerabilities, security breaches, and real-time news would require a central information repository for storage of news feeds and links to relevant security information. Formulas might be derived in Mathematica or other tools that are similar to econometric formulas with coefficients and weights that could describe a particular application or network behavior based on this data. If these formulas are effective at predicting a particular outcome (application or network behavior) they could be used to detect and prevent attacks.

Business Requirements for Security Analysis

The high-level business requirements for security analysis are research, scanning, monitoring, responding, and reporting security threats. Security tools help the IA (Intrusion Analyst) provide first line incident analysis and forensics as well as mitigate on-going attacks. At a lower level the business requirements

are the ability to filter and tune sensors to increase the confidence of valid attacks, determine if attacks are successful, the level of damage, repairing or reinstalling the system, auditing to verify repair, and determine what preventative processes and/or tools are required to prevent these attacks in the future.

Objective

The objective of this tool review was to review the current market of security tools and list some of the software tools that could provide short-term and long-term value for staff monitoring security systems. The links to the tool will provide some references to the technology functionality and provide a place to start in a review of security tools designed to help the security infrastructure. The tools will be intended to provide functionality to automate threat reporting and initiate incident analysis.

High Level Review Criteria

At a high level these tools should lower cost, manage change, and maintain quality for the enterprise IT operations and security staff enabling a high quality service for the enterprise user or customer.

Business Requirements

Security Dashboard

The security dashboard is a central point where all events from sensors are normalized and event correlation allows notification, reporting, and analysis of attacks detected by the sensors. The process of reading and filtering millions of events in real-time for analysis is centralized with the security dashboard and this eliminates time consuming review of many different data sources. Fast attack identification can result in mitigation or lower penetration levels of attack. The security dashboard will be a key tool in the initial creation of the service of attack enumeration. Some tools reviewed that provide some of the requirements of the security dashboard function are:

Netforensics: (www.netforensics.com)

Intellitactics: (www.intellitactics.com)

Symantec DeepSight Analyzer: (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=159&PID=13508394&EID=0)

Arcsight: (www.arcsight.com)

Attack Visualization

In order to provide a "big picture" of the current security events occurring within an enterprise network a depiction of copious amounts of security data into a 3-D image is extremely helpful. Due to the physical makeup of the human senses the eyes can retrieve and process huge amounts of data and process them much faster than all of the other senses. Visualization tools take network, application, and other types of events and provide a visual image of these events to help analysts review data and identify trends and correlations more quickly. This visual image can allow analysts to visualize millions of events in a picture that is organized in such a way to pinpoint new and existing attacks faster as well other information about sensor data. This quote from a paper by Philip Varner and John C. Knight supports this processing advantage human eyesight can provide in analysis by using what they call "preconscious mechanisms":

"The bandwidth of the human visual system is greater than any other sense, allowing humans to see and understand huge amounts of complex data quickly and accurately. A demonstration of this is the ability of a person to glance into a crowd of people and recognize a friendly face. With visual information processing, data is not only processed by the brain faster, but fundamentally changes our processing strategy. Instead of using conscious mechanisms (i.e. I read something, I translate it into a mental model, I understand the mental model), visual processing uses preconscious mechanisms. These mechanisms are "hardwired, highly parallel processes that handle the initial stages of analysis of the retinal patterns"[1]

This use of images to filter the monitoring data reduces the time (time=money) required by an analyst to find an attack or vulnerabilities. Some examples of tools providing this type of functionality are:

Secure Decisions: (www.securedecisions.com)

Silentrunner: (www.silentrunner.com)

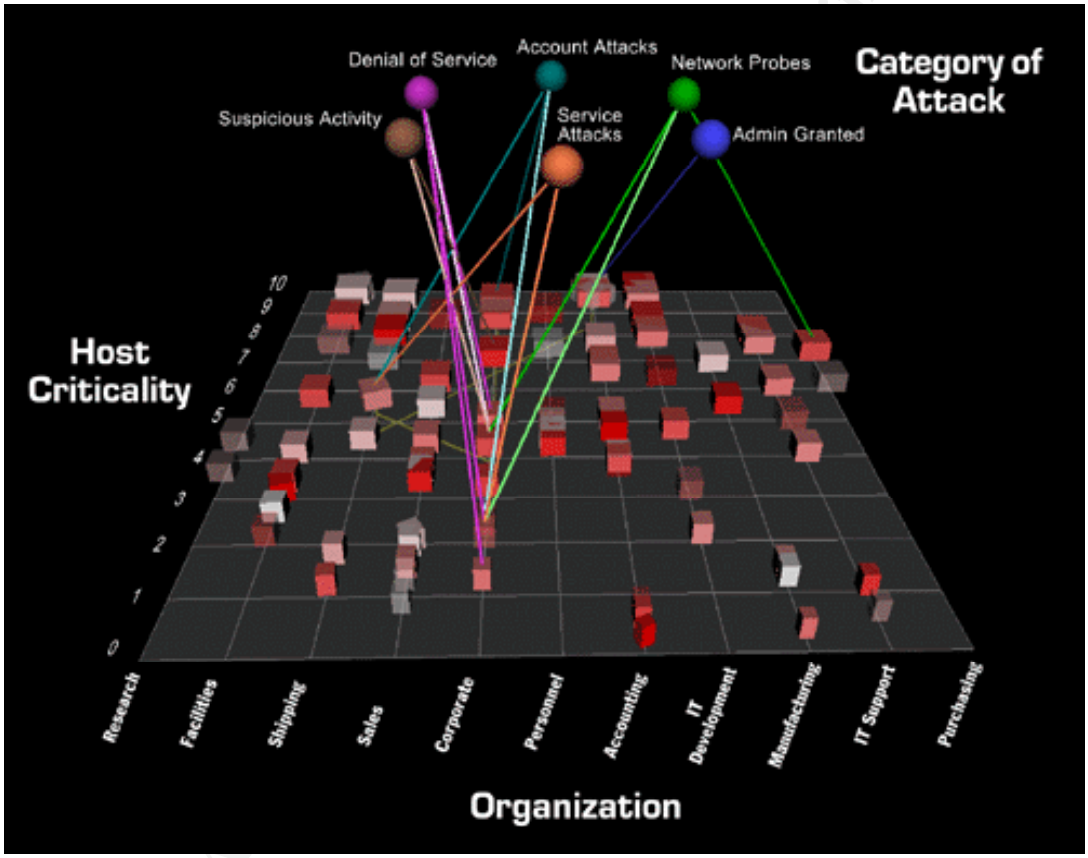
Lumeta: (www.lumeta.com)

Open Source OpenDX: http://www.opendx.org

---

1. Philip E. Varner and John C. Knight, "Security Monitoring, Visualization, and System Survivability: A Position Paper for ISW-2001" Department of Computer Science University of Virginia 8/10/2002 http://www.cert.org/research/isw/isw2001/papers/Varner-10-09.pdf

Secure Decisions software can depict many different relationships between networks and hosts and data can be organized visually to identify targets and sources of attacks. Many other "views" can be used for different security analysis purposes. Organizing views by process, source and destination addresses, user attributes like business department and other groupings provide answers to questions about the system behavior. Visualization can also provide information for network and application performance improvement. The benefit in the security space is that visualization makes it much easier to identify the attack as opposed to looking at large amounts of textual data where analysis for correlation will take more time. The use of 3-D planes can organize data in such a way that patterns emerge from alarm data.



[2]

Figure 1 - Secure Decisions

Profiling Applications

An ability to profile a specific application including network behavior such as listening, connecting, sending, and receiving data such as a testing or simulation environment to fully understand a specific application will help tune sensors and mitigate attacks. Specific device rules such as firewall settings

2 Secure Decisions, Inc. http://www.securedecisions.com/3-D_visualization.htm

could be created to permit or deny specific application behavior, perform logging, or start an alerting mechanism that could notify personnel or mitigate attacks. Network port information, process information, performance information, and other data could be simulated using software such as Opnet (http://www.opnet.com/products/modeler/) to understand application behavior and attributes. Network communication by applications could be analyzed using Netstat or better yet TCPview (www.sysinternals.com). Other tools to watch process trees to see which applications are spawned when executables run would provide valuable profiling information for possible Trojans and could help facilitate mitigation of threats.

Collaboration

Centralized groupware products with the capability to store many file types and provide a central information storage area would help analysts to access security information with data mining tools and automate the collection of security meta-data. Functionality such as role based user ACL's, workflow, advanced search and correlation capabilities would be required to reduce the time spent searching for information. The repository could provide collaboration for decision-making, issue resolution, version control, remote decision-making, and staying up to date on security events worldwide. There are freeware products and commercial products available. Software like IBM's Lotus Domino (http://www.lotus.com/products/r5web.nsf/webhome/nr5serverhp-new) and other repositories like Documentum (www.documentum.com) for documentation accessed by web browser provide this functionality. Another web-based collaboration tool is Eroom which (www.eroom.com) could provide this integrated group collaboration functionality within enterprise security analyst teams.

Security Policy Generation and Compliance Management

Tools to create and manage multiple custom security policies and perform basic quality assurance tasks would save time Policies will need to change over time due to new business rules, risk management decisions, new applications, IDS rules, threat mitigation rules, and many other reasons. The ability to reduce time spent managing policy and insuring compliance to the policy will be critical to security service provision and reduction of administration costs. An example of software to provide this functionality would be PentaSafe (www.pentasafe.com) or Symantec's product Enterprise Security Manager: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=45&PID=13512357&EID=0.

Business Requirements for the Security Dashboard Tools

Import Data from New and Existing Devices

Tools must provide the ability to receive alert data from other software and integrate alerts from devices including PC event logs, syslog data, and IDS data streams. Ability to receive data feeds from Cisco, Checkpoint, and leading IDS products such as SNORT, Entercept, and data archived in TCPdump format would be a requirement. HIDS tools, firewalls, event logs, and router data are only a few of the device data that should be able to be imported and summarized from heterogeneous devices.

Alarm Normalization

The data that is imported would need to be normalized into one database so correlation of data such as vendor specific severity rankings, source and destination IP addresses, time of event, and many other data points can be correlated to find trends indicating source or type of attack. Normalizing the alarms from different devices allows comparisons between different devices with independent alarm severity scales. This creates the ability to "rank" the attack in severity across devices defined by ability to damage, ability to spread, and other factors. This ranking ability would provide the ability to categorize and prioritize the IA response to attacks and to queue security cases for forensic investigation.

Event Correlation

Event correlation describes the ability of the security dashboard product to review real-time and historical data in a normalized database of events and trigger rules that look for events that match specific criteria indicating an attack or vulnerability. Rules would represent an attack type with specific network criteria such as specific ports and protocols, known content strings in malware, or specific packet header data. Rules using data from multiple devices increases the confidence of the event being a real attack. Event correlation provides the ability to query millions of records and filter these records from "normal" events and find anomaly events that could indicate an attack. Event correlation provides an additional checkpoint in intrusion analysis. It might decrease the time to learn about a specific network and the false positives for that network so that the actual events that signal an attack for that network can be discovered faster than if an analyst was reviewing the normalized data manually. Here is a comment by Dennis Drogseth describing how event correlation can help determine the root cause of an event or set of alarms

"*Event correlation is the process of correlating alarms to isolate the point of failure. When it's thorough, event correlation may yield root cause analysis - which provides the single identifiable cause of a problem. Mere alarm suppression provides, by comparison, only a partial answer to the problem - reducing the number of alarms generated by a failure so the person trying to fix*

the problem isn't overrun by alarms that are of less consequence."[3]

Extensibility – Trigger Other Applications

The security dashboard product needs the ability to trigger other tool sets to perform functionality such as additional more focused intrusion analysis through filtering logic and additional data gathering for forensics. The ability to add links to the executables for centralized execution of tools would centralize access to these tools for the analyst. Examples of tools to execute automatically or manually might be ping, traceroute, finger and other commonly used tools such as Nessus or NMAP for vulnerability scanning.

Forensics Management

Functionality within the security dashboard should provide the ability for forensic case assignment and prioritization in order that investigations may be prioritized and escalated per business requirements of the enterprise. The metrics regarding these investigations will provide feedback on workloads, compromises, and areas to improve security policy.

Reporting

Deep attack reporting would be a requirement including many commonly known attack types and the ability to export data to tools such as Crystal Reports for integration with sensor alert data. Scheduled and Ad-Hoc reports should be available via web browser access or email attachment and can be customized.

Continuous Improvement

Provide an intuitive GUI for the discovery process of relevant attack information and quickly identify "critical" events that are relevant to an investigation and provide the ability to store those for future use in the intrusion analysis. Use best-known methods today for intrusion analysis and incorporate new BKM's that would help improve the enterprise security service.

Customized Event Correlation Rule Creation

The event correlation functionality is only as good as the existing rule set and the

[3] Dennis Drogseth," Why it may be time to invest in event correlation (if you haven't already)" Network World on Network/Systems Management*, 07/26/99*

ability to create custom rules to trigger event correlation for sensor alerts is a requirement for a security dashboard to provide new attack detection. The simplicity and robustness of the rule creation engine and language will be important. Also the ability to create rules for notification and reporting functionality would be very important.

Categorized Security Tools List

Tool Links Categorized by Business Function

These are links to many of the tools reviewed and this list will definitely get outdated over time but will provide some product information at least in the short term (2002-2003):

Tool Link	Tool Category
http://enterprisesecurity.symantec.com/article.cfm?articleid=1540	Dashboard
http://www.itactics.com/	Dashboard
http://www.netforensics.com/	Dashboard
http://www.securesoftsystems.com/	Dashboard
http://www.intrusion.com	Dashboard
http://www.opensystems.com/index.asp	Dashboard
http://www.micromuse.com/	Dashboard
http://www.open.com/htm/products.htm	Dashboard
http://www.freshwater.com/SiteScope.htm	Dashboard
http://www.esecurityinc.com/	Dashboard
http://www.advisortechnologies.com/Products.htm	Dashboard
http://www.aprisma.com/products/security.shtml	Dashboard
http://www.trustworks.com/home/content.html	Dashboard
http://www.pentasafe.com/	Dashboard
http://www.riptech.com/index.html	Dashboard
http://www.counterpane.com/ontheday.pdf	Dashboard
http://www.arcsight.com	Dashboard
http://www.network-1.com/website/products/centralized/centralized.asp	Dashboard
http://www.iss.net/products_services/enterprise_protection/rssite_protector/siteprotector.php	Dashboard
http://desidrta.uta.edu/	Security Subsystem
http://www.netlock.com/product.html	Security Subsystem
http://secinf.net/info/ids/nn-idse/	Security Subsystem
http://www.intersectalliance.com/projects/index.html	Security Subsystem
http://www.estpak.ee/~risto/sec/	Security Subsystem
http://www.nfr.com	NIDS
http://www.snort.org	NIDS – Snort open source IDS
http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html	NIDS – Cisco IDS
http://www.iss.net/products_services/enterprise_protection/rsnetwork/gigabitsensor.php	NIDS – Gigabit Sensor
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=156&PID=13508106&EID=0	NIDS – Manhunt

http://www.sourcefire.com	NIDS – Commercial version of SNORT
http://www.entercept.com	HIPS – Web, SQL Server, and standard editions
http://www.iss.net	HIDS – BlackICE, Real Sensor
http://www.enterasys.com/ids/	HIDS - Dragon
http://www.tippingpoint.com	NIPS
http://www.intruvert.com	NIPS
http://www.stillsecure.com/index.html	NIPS
http://www.dshield.org	DIDS
http://www.incidents.org	DIDS
http://aris.securityfocus.com/	DIDS
http://www.mynetwatchman.com/	DIDS
http://www.messagelabs.com/viruseye/	DIDS
http://www.eeye.com	NIDS/Scanners

Analyst Support

The analyst needs to protect the consumer or end user who uses the enterprise network, Internet, and uses VPN connectivity to access corporate networks and hosts. The analyst does this by using tools that enforce security policy such as firewall rules which allow the analyst to stop specific network traffic by protocol, source IP, destination IP, thereby mitigating a threat. The security dashboard tools will support the analyst's focus on protecting the enterprise in a more efficient manner.

To mitigate threats the data returned in alerts and TCPdump logs must provide useful information to make tactical decisions and drive new security policy enforcement through dashboard information analysis and synthesis. This process may be somewhat manual or fully automated depending on attack type. It is best to have an analyst make a decision instead of using tool based active response to block attacks. Active response could be used against you in a DoS attack if automated. In some cases active response makes sense if it is deployed in a manner that cannot be used against the enterprise such as when used in conjunction with white lists. An example of what not to do would be setting up a NIDS system to automatically install ACL's on a router to block the source IP address of an attacker. The packets involved with the attack would most likely have "spoofed" IP addresses that are the not same as the attackers actual source IP address. An attacker could forge packets with the root DNS servers as the attackers source IP address. If active response were activated to block all root DNS servers all Internet service for email, browsing, or any other

service requiring the use of DNS would be effectively stopped. But an active response setup to block access to a router except for predefined IP addresses might be an effective way to block attempts to login to a router by an attacker. So, a human making informed decisions and weighing the risks of active response and configuring these features where appropriate is an essential function of the analyst.

Summary

There appear to be definite benefits such as better overall ROI on security investment in HIDS, NIDS, firewalls, and other security tools by deploying a central security dashboard including tools such as visualization software, security policy generation, application profiling, and collaboration tools to improve monitoring accuracy, workload, reporting, and analysis. The problem of information overload may still exist but it can be managed much better. Tools that have the ability to prevent attacks are beginning to become available so simply monitoring the environment is not enough. Automatically executing tools to do forensics, applying new rules on devices to stop attacks in real-time, and capturing evidence for prosecution can be automatic but use of these features needs to wait until security tools mature. The state of security tools deployment is changing and at the time of the creation of this document a mid-size or small enterprise would probably be better off outsourcing the centralized security monitoring function to an MSSP that will already have these expensive security dashboard tools and the expertise to use them intelligently. As the tools come down in price enough to justify the deployment, training, and administration cost of ownership small to medium sized firm may start deployment due to the better ROI. In short all organizations need to look at the central monitoring dashboard as a part of their overall security strategy now but cost is very much a determinant in deployment.

Appendix A – References

1. Philip E. Varner and John C. Knight, “Security Monitoring, Visualization, and System Survivability: A Position Paper for ISW-2001” Department of Computer Science University of Virginia 8/10/2002 http://www.cert.org/research/isw/isw2001/papers/Varner-10-09.pdf

2. Dennis Drogseth,” Why it may be time to invest in event correlation (if you haven't already)” Network World on Network/Systems Management, 07/26/99

3. John Q. Walker, Ph.D., NetIQ Corporation “Security Event Correlation: Where Are We Now?” http://activeanswers.compaq.com/aa_downloads/6/100/225/1/53668.pdf 7/22/2002

4. George V. Hulme, “Security systems generate an overload of information. New tools help manage it all more effectively.” InformationWeek.Com http://www.informationweek.com/story/IWK20020816S0036 Aug. 19, 2002

5. David Freeman, “Information War-fare,” MIT Technology Review, volume 104, number 9, pages 61-67, November 2001, http://www.technologyreview.com/articles/freedman1101.asp

6. Ruttrell Yasin, “Security Mandate: Silence False Alarms,” *Internet Wee*k, April 8, 1999, http://www.internetwk.com/story/INW19990408S0009

7. Alarm Management Standardization: http://www.ietf.org/html.charters/disman-charter.html

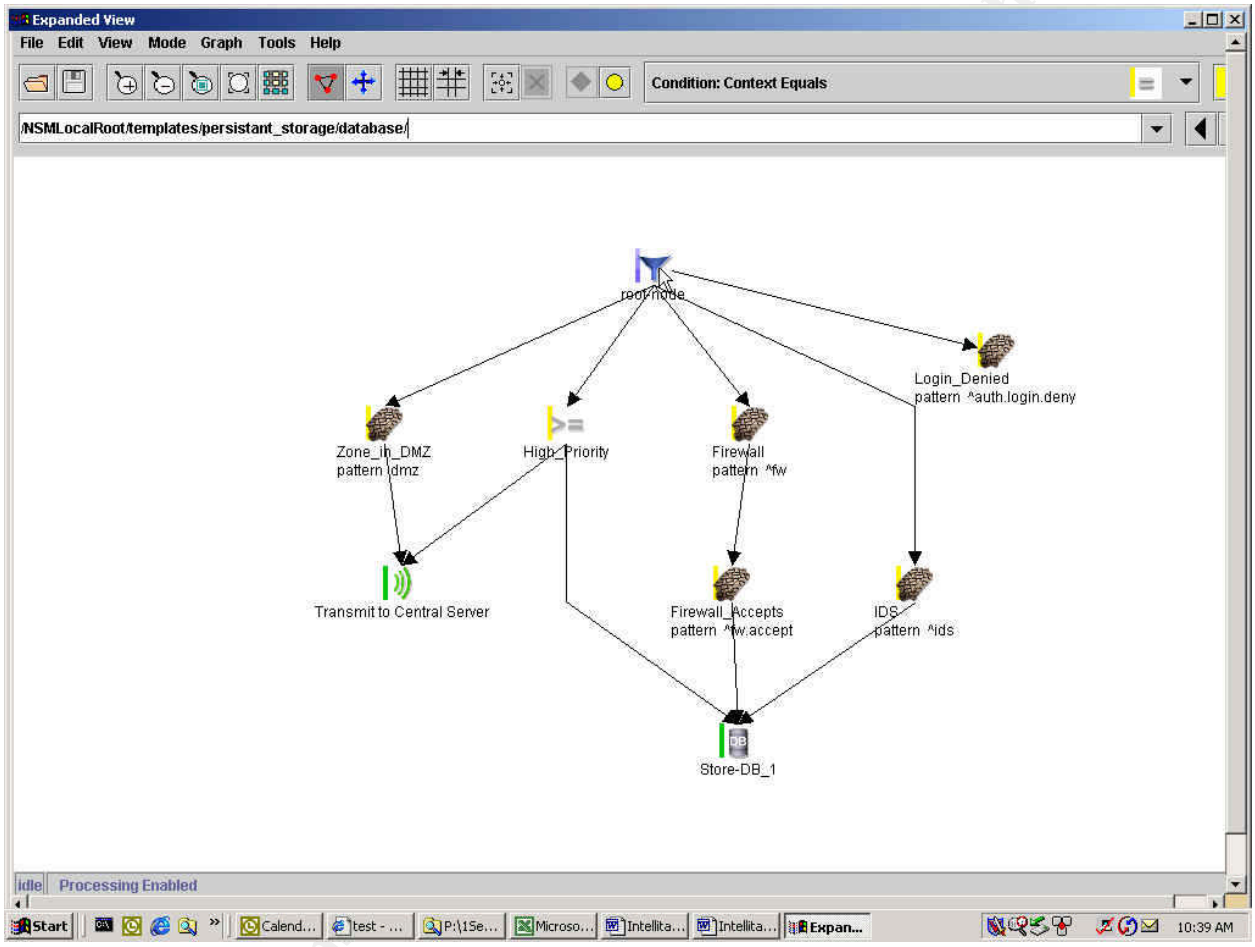
8. Colby DeRodeff, ArcSight, Inc. “Got Correlation? Not Without Normalization” Arcsight 2002 http://www.arcsight.com/graphics/product/NormCorr.pdf

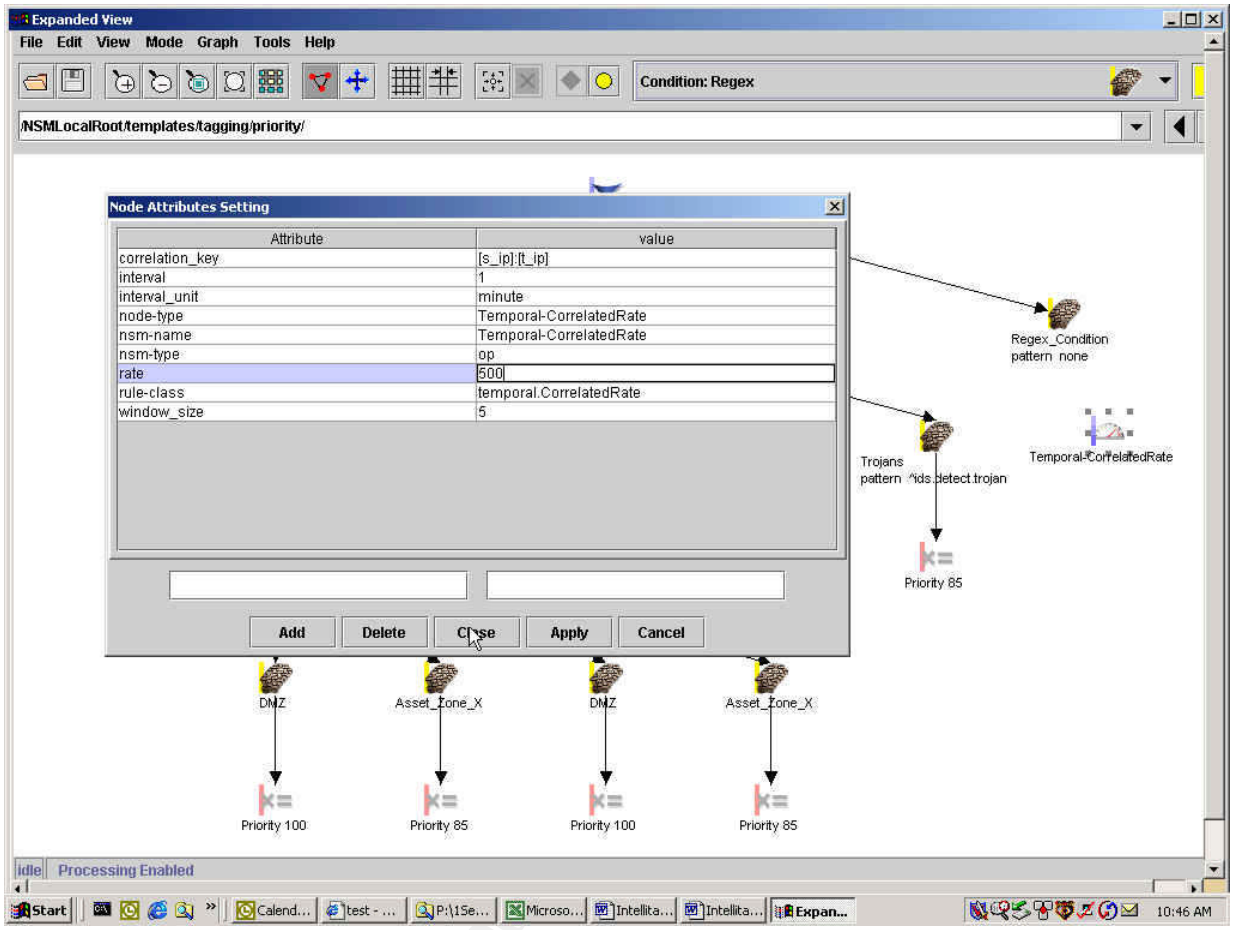
9. Denise Dubie, “Users shoring up Net security with SIM”, Network World 09/30/2002 http://www.nwfusion.com/news/2002/0930apps.html

10. Ellen Messmer & Denise Dubie, “SIM attracting new players, rivalries”, Network World 09/30/2002 http://www.nwfusion.com/news/2002/0930sim.html

Appendix B – Examples of Security Dashboard GUI's

Intellitactics Screenshots





Arcsight Screen shots