Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Design and Theory of Data Visualization Tools and Techniques

Networked enterprises have grown exponentially for more than a decade and have become quite unwieldy to manage and secure. What we now have are massive heterogeneous environments that offer, and demand, extensive resources and bandwidth. Thus, many of our existing tools are no longer viable for managing these networks. However, there are many new tools, techniques, and approaches on the horizon that have the potential to scale to, and with, the enterprise. One such technique is that of rendering a visual representation...

Copyright SANS Institute

Author Retains Full Rights

AD

Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Intrusion Detection in Depth

GIAC Certified Intrusion Analyst (GCIA) Practical Assignment

GCIA Practical Version 3.0
SANS 2001 Washington DC

Brian K. Sheffler

© SANS Institute 2002, Author retains full rights.

Assignment 2

An Approach to Intrusion Analysis

The Design and Theory of Data Visualization Tools and Techniques

The purpose of this paper is to inform and educate security professionals about the analytical potential of using a tool or technique that renders visual representations of the data/traffic that traverses a given network. The emphasis is on the design and theory behind such tools. Included are examples of data visualization products that are commercially available.

© SANS Institute 2002, Author retains full rights.

Introduction

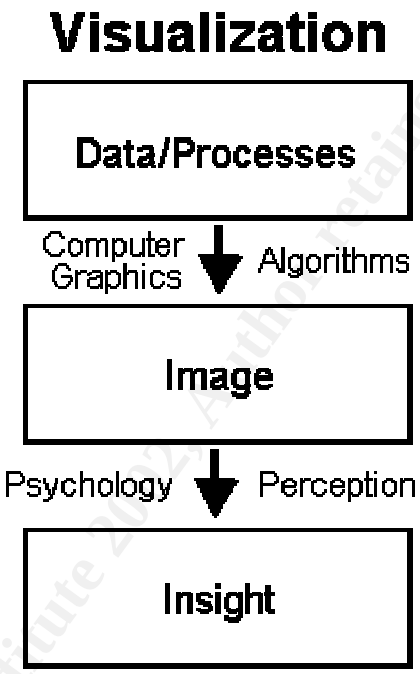
Networked enterprises have grown exponentially for more than a decade and have become quite unwieldy to manage and secure. These issues stem from the rapid development and implementation of technology over a short period of time. What we now have are massive heterogeneous environments that offer, and demand, more resources and bandwidth than ever before. Thus, many of our existing tools are no longer viable for managing these networks. However, there are many new tools, techniques, and approaches on the horizon that have the potential to scale to, and with, the enterprise. One such technique is that of rendering a visual representation of data for the use of inter-network traffic analysis. It is primarily my personal experience with the limitations of existing products that has prompted me to further explore the design potential of the data visualization approach.

Edward Tufte, a pioneer in the use of graphics as a means of representing information, argues that a major issue we deal with is that of presenting large amounts of information in a way that is compact, accurate, adequate for the purpose, and easy to understand. Specifically, to show cause and effect, to insure that the proper comparisons are made, and to achieve the (valid) goals that are desired. He further states that the solution is to develop a consistent approach to the display of graphics, which enhances its dissemination, accuracy, and ease of comprehension.[1] And although traffic analysis was not necessarily his intent, this approach can be applied to the data visualization techniques and tools that are being developed for this specific purpose.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Basis for Design and Use

To begin the design of a tool or technique you must first define the processes involved and the relationship between those processes. Khai Truong, Gregory Abowd, and Jason A. Brotherton, of the College of Computing & GVU Center at the Georgia Institute of Technology in Atlanta, Georgia defined the process of *capture and access* as "the task of preserving a record of some live experience that is then reviewed at some point in the future. Capture occurs when a tool generates an artifact that documents the history of what happened and access devices are the tools used to review the captured experiences."[2] Furthermore, a true science of visualization must incorporate both a formal theory of computer graphics and a theory of human perception.[3a]



*From URL: http://www.ergogero.com/dataviz/dviz1.html[3a]

In intrusion analysis our capture devices are made up of intrusion detection devices (IDS) and the logs from other attached networked devices/applications. The collection and structuring of these captures is how we make the access to this stored data available for review and analysis. This is often done by collecting the captures in a database that is indexed for the timely retrieval of the stored data. The idea behind data visualization in traffic analysis is that the data may be presented to the user in a format that is optimized for ease of comprehension, and to make identifying anomalous traffic and patterns more easily recognizable. A prime benefit of being able to visualize these captures is that the new perspective often lends itself to revealing hidden patterns that may not be readily apparent from the context of a flat file or queried result. Also, the efficiency with which we can perform analysis on large amounts of data can be increased, thus maximizing those resources required when performing that analysis. Therefore, "designers constructing capture and access applications are faced with more than just issues related to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

different pieces of data. Beyond data, there are still the users, the devices, time and locations involved in the experience to take into consideration in the design."[2]

"These components form the minimal set of issues that need to be addressed when designing capture and access applications:
- *Who* are the users?
- *What* is captured and accessed?
- *When* does capture and access occur?
- *Where* does capture and access occur?
- *How* is capture and access performed?"[2]
- *Why* data visualization?

The Who Dimension-

"In understanding each person's part, designers can design systems to support specific roles in the capture and access of the experience."[2] For example, within the network and systems security arena, we have Administrators, Managers, Incident Handlers, and Intrusion Analysts, among others, who may all be a part of the "system" that is used to provide protection for a given network. Because these roles may somewhat overlap, but have different means and motivations, the design of a given tool or technique must be cognizant of those requirements that are levied by each of this supporting cast. Otherwise, the tool may be no more beneficial than those that are already in use and may just add overhead to an already time and resource intensive process.

"The issues in the *who* dimension that designers must consider are:
- The number of capturers
- The number of accessors
- The overlap between capturers and accessors
- The perspective of the capture (public, private, shared, etc.)"[2]

The What Dimension-

"Designers must also identify *what* to capture and make available for access; that is, determine what artifacts best document the experience. While the actual experience sets the ceiling for what is captured, the amount of information actually captured sets the ceiling for the access of the experience." "To increase the fidelity of the access experience, more streams can be captured and integrated; collectively, they can give a more accurate account of the experience."[2] The *what* portion of the design process tends to focus on the collection, or capture, of the data of which, from a data visualization standpoint, is often determined by the type of output that your particular IDS/log file uses. In network security, my experience is that we try to capture everything we possibly can, and that our greatest limitation for collecting data is either the monetary resources that have been committed to a security operation or the scale of the operation/enterprise that we are trying to protect. These issues will be discussed further in the Limitations section of this white paper.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

What is of direct importance though, in visualization, is that the interface, or access, between the visualization tool and the stored captures is flexible enough to accept any format of data, to include data from multiple sources. It must also do this without seriously inhibiting the timeliness of the rendered output. If the tool is too cumbersome or resource intensive then you may limit the amount of manipulation that is possible with the rendered result. The capability of manipulating the data is the key to making a visualization technique an integral and useful part of an Intrusion Analysts repertoire.

"The issues in the *what* dimension that designers must consider are:
- The artifacts in the live experience
- The artifacts captured
- The artifacts accessed
- The fidelity of the access experience with respect to the live experience"[2]

The When Dimension-

"The *when* dimension deals with issues related to when capture occurs, when access occurs, and the time scale between the capture and access phases."[2] This is where we, as Intrusion Analysts and Incident Handlers, continue to demand that the capture and access devices we use provide that captured data in an environment that is as near to real-time as possible and archive that data for as long as possible. This is because the security of our networks and our approach when responding to a possible intrusion is directly related to the time and timeframe in which that traffic occurs.

"… Long-term applications store information as records for posterity. Information needs to persist for much longer periods of time than other types of applications and it may make sense to provide users with a synthesized summary of the experience with an interface that supports being able to drill down to the exact point that the user(s) want to review."[2] This "drill-down" feature would be extremely beneficial to those Handlers and Analysts that must support a large enterprise that passes enormous amounts of traffic, but may not have the manpower and resources available to perform a full, in-depth analysis of all traffic. This visual overview of network traffic can be an efficient and helpful way to identify those anomalous events that are of the highest criticality to your overall network security. But of note is that by generalizing, or aggregating, the data you may distort the fidelity and accuracy of the detail that often only exists in the more raw forms of the original data. Those details are often what are necessary in order to perform an accurate analysis of network events. That is why it is important to retain, and make available, as much detail as possible when drilling down into an event. However, most of the visualization tools I have dealt with perform their rendering based on how the data is presented to the visualization tool and any generalization, summarization, or aggregation that is performed on the original data is most often implemented by the collection or access device, not by the visual rendering tool itself. Therefore, the adverse affects of generalization are most likely to be symptoms of your collection/access devices and may be overcome through a well, thought out security strategy. However, due to the previously indicated requirement for long-term storage, some operations may be bound by the limitations of those collateral systems that support the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

underlying security infrastructure. This is to say that although data visualization is a most helpful tool for many varying circumstances, it is not a "silver bullet" and must be applied in the correct manner in order to be effective. A lesson learned from this is that you should never become reliant on any one tool when performing analysis. Correlation is a key ingredient in any analysis, and security is no exception. Just like any other tool, it should be one of many that aid the analyst in the performance of his or her duties.

"The issues in the *when* dimension that designers must consider are:
- The times when capture occurs
- The times when access occurs
- The frequency/periodicity of the capture and access occurrences
- The time scale difference between when capture and access happens"[2]

The Where Dimension-

"The *where* dimension addresses the physical locations involved in capture and access phases. Most capture and access applications handle experiences that occur in a single location. However, it is becoming more commonplace for people in many different places to collaborate and essentially share an experience remotely. Furthermore, capture and access applications must also take user mobility into consideration."[2]

Visualization of the *where* provides an excellent technique, by perspective and from a temporal display, for viewing the distribution and time-line of traffic and events that occur across an enterprise. Identifying where traffic and attempts occur can help inform the analyst of the magnitude or scope of an event, of potential distributed attacks, and of possible weaknesses in their security posture. These are some of the greatest advantages of using data visualization, versus that of a standard database or flat file, when performing intrusion detection and analysis.

"The issues in the *where* dimension designers must consider are:
- The locations of capture
- The locations of access
- The overlap of physical spaces
- The mobility of the users
- The multiplicity of locations"[2]

The How Dimension-

"The tools and methods for capturing and accessing information as well as the scale of devices form the last dimension: *how*. Capture and access applications are typically built as a confederation of tools. The number of devices that are used in a system defines the scale of devices for capture and access applications. At one end of the scale, only a single device is used in the application. A key question in the building of capture and access devices is whether the device that is doing the capture can also be used to provide the access." "In most cases, capture

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

is often done using a number of devices and so a certain amount of effort must be devoted to coordinating these devices to work together."[2]

In this dimension the integration of the devices involved, along with the users, takes center stage. Here the numbers, locations, roles, and capabilities of the various devices must all be developed into a comprehensive and intuitive interface that is also robust and stable. The *how* of any security system may be the most complex stage of the technical design and its utility. Furthermore, when creating a visual representation of data the execution and sustainability of an application becomes that much more complex due to the additional overhead and resource requirements. This is important because the fidelity and integrity of one's resulting analysis will only be as accurate as the amount and timeliness of their data. For example, if you only capture 50% of your network traffic, or your systems are unavailable/unreliable 50% of the time, then so to will be the accuracy and timeliness of your analysis. Thus, the perceived usefulness, or trust, that the Analysts and Handlers place on the tool will be directly related to the successful implementation of these previously referenced dimensions.

"The issues in the *how* dimension designers must consider are:
- The method of capture
- The number of capture devices
- The number of access devices
- The role of the devices"[2]

The Why Dimension-

I have added this dimension to the design process because it is truly the driving force behind data visualization in traffic analysis. The Why is the justification and value-added portion for the practical application of this technique. The following statement summarizes the Why dimension of data visualization: Analysts need a tool that can aid them in determining whether something *counter-intuitive* is, or has, occurred. Hence, the Holy Grail of intrusion analysis. For it is not what we know, but what we don't know, that often concerns us the most.

The issues in the *why* dimensions include:
- Why develop data visualization tools/techniques
- The usefulness of the tool/technique
- The benefits of the tool/technique
- The practicality/feasibility of implementing the tool/technique

© SANS Institute 2002, Author retains full rights.

Limitations of Existing Designs

From the dimensions and issues discussed this far, one can begin to grasp how the complexity of visualization has inherently led to many of the limitations that exist in today's commercial products. However, because these principles have progressed from a preset of initial concepts, their continuing evolution has provided a fairly thorough set of guidelines for structuring the next generation of visualization tools. Initially, many of the current products were developed as proofs-of-concept due to the stated complexity and under-perceived practical application in various fields. But, when, and where, open integration and the application of these sound design standards take focus those ensuing tools will begin to benefit many fields beyond that of the classroom and traffic analysis environments.

The first of the three greatest limitations that currently inhibit existing data visualization products is that of resources. Because data visualization products are fairly young in their development cycles, many are very resource intensive and inefficient. I have personally experienced this while running one such tool on a dual Pentium 4 Xeon processor server with 1 GB of memory, mostly when rendering medium-to-large quantities of data, or when rendering data in 3-D. This contributes to the high cost of such tools, as does the learning curve that is associated with any new application. Because this is a tangible limitation, it is also the most easily overcome. However, the money and expertise required at this stage are prohibitive to widespread implementations of these tools. The costs associated with these tools will recede over time, as will the learning curve, but until then, justifying the Why dimension's questions of feasibility and practicality will be based mostly on the potential and scalability of the tools usefulness in a given environment.

The second limitation to note is that of integration and interoperability. Herein lies the fabric that brings the concept to the desktop. Due to past experiences with different tools, the integration with the capture/access device is of extreme importance when choosing or designing a tool. Some of these tools are able to import data from a flat file, while others only accept data from a limited range of commercial vendor databases. Most of them can be ported or customized to the requirements of a given customer, however, this then leads you back to the first limitation of cost and feasibility. Those organizations with developers on staff may be able to overcome some of these issues internally, as has mine, but again, this will deter the adoption of visualization tools for many smaller enterprises. Besides the issue of accessing the data is that of defining and representing the data in a meaningful structure. Here I must give credit to those vendors whose tools I have used, because they all seem to be very flexible and with out many restrictions in this regard. However, most existing tools work with the assumption that an IDS or application has already performed some type of once over analysis that allows for the visualization of the pre-munged data. Because this scenario is probably true more often than not, I can not fault them for this decision, but security professionals should be aware that adapting raw or unaggregated data can be quite cumbersome and complex, once again degrading the feasibility in some environments.

The final and often most important limitation is that of the human factor. These are the limitations that will most affect the final design and capability of any visualization tool. These issues can only be addressed up to the point that we, as human beings, possess the ability to gain

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

meaning from a visual stimulus. "For human beings, our potential is directly constrained by our attention, memory, and processing capabilities."[3b] From this perspective, we tend to have difficulty dealing with and processing information that exists visually in more than three-dimensions. Thus, many tools are governed by what is assumed to be the ability of the customer. This is not a limitation that necessarily has a solution or, if one does exist, will be easily overcome. Alas, we are our own weakest links… but, never underestimate human ingenuity.

Tool and Theory Overview –

The most compelling reason for using data visualization in analysis is that of resources. Due to the scale of many enterprises, there are not enough intrusion analysts, nor is there enough time, available to cover all of the networks that are in existence today. And, at the rate the Internet and networks are expanding this trend is not likely to go away.

Although I originally started writing this paper because of my personal experiences in intrusion detection and my frustration with some of the tools that are available to analysts, my learning experience while performing the research for this paper has afforded me new insights about the challenges we face. For those of us working in large enterprises, the tools that we currently use are quickly becoming outdated and overburdened. Because the possibility of hiring more, highly qualified analysts is not always an option, new tools and techniques must be developed that allow us to maximize those resources we do have access to.

We must become conscious of the amounts of time we can allocate to analyzing traffic and detects. If we are able to investigate, or capture, 1 out of every 10 detects, then that means there are potentially 9 incidents that may go unresolved. Our goal should be to bring that number to 0, even though this may not be truly possible. In large or global enterprises, we need tools that can help us find patterns and perform correlation in a fast and effective manner. Currently I believe that a great amount of potential for doing just that exists by utilizing data visualization techniques. Postmortem analysis is a reactive process that does nothing to defend against ongoing and new/original attack methods. Through near real-time data visualization, the analysts can observe what is happening around them as the activities occur, and they can see this from different perspectives and at different levels. Databases queries and flat files are not currently capable of providing this level of hierarchical analysis form the top down. That is why I am a sincere advocate of developing technologies that allow for the near real-time visualization of network traffic for the purposes of security and management.

Currently most of the analysts I know of, that are using some sort of data visualization tool, are using it reactively to find patterns and anomalies from within sets of raw data. Herein lies another great strength of visualization. Because of the capability to view data on multiple axes, an analyst can see traffic as it occurred across time and locations, while at the same time having the data sorted by event categories and system/network roles, in conjunction with correlating between multiple source IPs.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Listed in the appendices of this assignment are examples of some data visualization tools that are commercially available. Once these tools and techniques mature, then near real-time analysis, along those lines indicated above, should become a reality. This is the direction in which, I feel, intrusion analysis/detection should be moving.

Recommended Reading –

For further information on the origin, concepts, and design of general visualization techniques:

- "The Visual Display of Quantitative Information" by Edward R. Tufte (Graphics Press); ISBN: 096139210X.
- "Envisioning Information" by Edward R. Tufte (Graphics Press); ISBN: 0961392118.
- "Visual Explanations: Images and Quantities" by Edward R. Tufte (Graphics Press); ISBN: 0961392126.
- "Readings in Information Visualization : Using Vision to Think" by Stuart K. Card, Jock D. MacKinlay, and Ben Shneiderman (Morgan Kaufmann Publishers); ISBN: 1558605339.
- "Designing Visual Interfaces: Communication Oriented Techniques" by Kevin Mullet and Darrell Sano (Prentice Hall) ; ISBN: 0133033899.
- "Ultimate Visual Dictionary 2001" (DK Publishing); ISBN: 0789461110.
- "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond" by Marc Green, Ph.D.; URL: http://www.ergogero.com/dataviz/dviz0.html.[3]

© SANS Institute 2002, Author retains full rights.

Appendix A

Visual Insights' ADVIZOR™

The following is an excerpt from an informational document (.pdf) titled "ADVIZOR™: A Technical Overview" which was authored by Stephen G. Eicks, Ph.D., of Visual Insights, Incorporated (www.visualinsights.com). The document can be downloaded from the following web site:

http://www.visualinsights.com/pressroom/whitepapers/advisor_tech.pdf[4]

Although I downloaded the file on 21 January 2002, I was unable to determine when it was actually written/published. However, the information it contains is relevant and supports the objective of this practical.

Overview –

"Visual Insights ADVIZOR is a flexible environment and platform for building interactive visual query and analysis applications. ADVIZOR consists of four parts: a rich set of flexible visual components, an in-memory data pool, data manipulation components, and container applications. Working together, ADVIZOR's architecture provides a powerful production platform for creating innovative visual query and analysis applications.

Visual Insights' ADVIZOR™ is a complete interactive environment for building visual applications. Analogous to a "visual spreadsheet," ADVIZOR enables companies to add visual query and analysis solutions to their existing decision support infrastructure. Systems now routinely collect fine-grain transaction data. By analyzing this data, i.e. understanding customer buying decisions, exploiting cross-sell opportunities, better managing brands, and leveraging limited shelf space, businesses can achieve significant advantage. The analysis tools, unfortunately, have not kept pace with ever increasing data volumes. The result is data overload and information drought, the inability to make effective business decisions because of too much data.

The idea embodied in ADVIZOR is that desktop PCs, including browser-based thin clients, have become fast enough to enable a new class of analysis and query tools that exploit interactive visualization. Previous approaches to making sense of data involved manipulating text displays such as crosstabs, running complex statistical packages, and assembling the results into reports using presentation graphics. Browsers and the web have popularized the idea that modern interfaces combine text and graphics. ADVIZOR takes this approach one step further by making the text and graphics interactive, applying color to encode information, and enabling the user to pose and resolve queries dynamically using the mouse. Broadly speaking, visual tasks may be divided into three classes.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

1. *Presentation Graphics* such as is included with MS PowerPoint or even spreadsheet graphics. These generally consist of bars, pies, and line charts that are easily populated with static data and drop into printed reports or presentations. The next version of presentation graphics, exemplified by VRML-based browsers, enriches the static displays with a 3D information landscape. Users can then navigate through the landscape and animate it to display time-oriented information. This class of visualizations is generally useful for answering "what" questions and for conveying results.

2. *Visual Interfaces* for Information Access are focused on enabling users to navigate through complex spaces such as the web and find nuggets of information. Supported user tasks involve searching, back tracking, and history logging. User Interface techniques attempt to preserve user context and support smooth transitions between locations.

3. *Full Visual Query and Analysis* systems such as ADVIZOR that combine the excitement of presentation graphics with the ability to probe, drill-down, filter, and manipulate the display to answer the "why" questions.

The difference between answering a "what" and a "why" question involves an interactive operation. For example, in a set of sales data the answer to a "what happened" might be that sales went up. Answering the why question might involve an interactive operation such as drilling-down, drilling-across, hiding, or rescaling to discover that one product had an exceptional quarter. Both of these are "single table" questions since they can both be answered from a data table showing sales by product. Going further requires linking multiple data tables, e.g. relating the sales table to the transaction table. It might be that sales went up because of a single huge order. For a busy analyst it is important to provide fast and efficient techniques to navigate through the many varied possibilities."[4]

Summary –

"There are three unique and compelling aspects to ADVIZOR's technology:

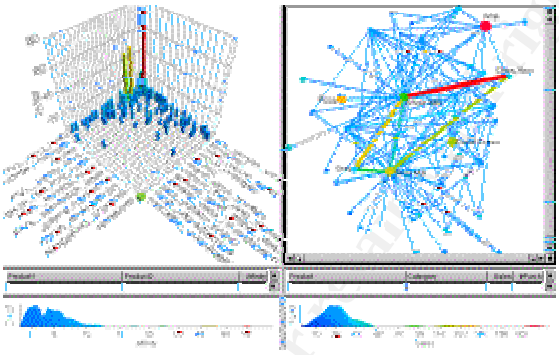
- Rich interactive Visual Components that are linked by selection, focus, data, and color
- Data Pool containing multiple, linkable tables for visualization
- ADVIZOR and ADVIZOR/2000 containers that host the components and function as visual workspaces.

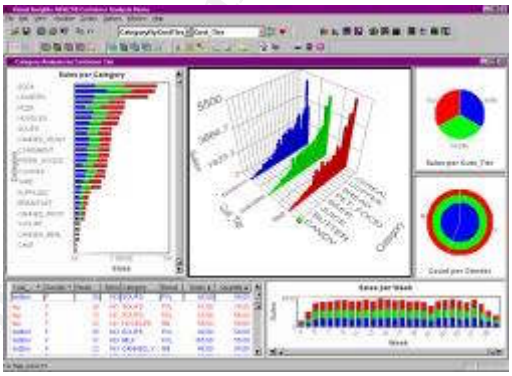
Together the different aspects of ADVIZOR function as a powerful environment for visual query and analysis."[4]

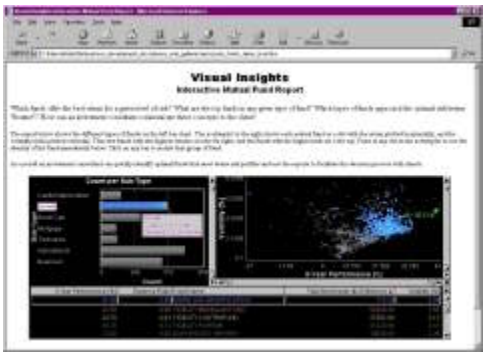
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Screen Captures –

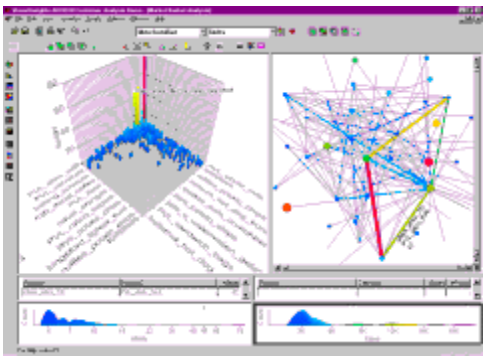
The following screen captures can be found at the Visual Insights web site: http://www.visualinsights.com/base_pages/mainhtml.asp?level1=four&level2=three&level3=one&picked=4-1-1[5]







© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



© SANS Institute 2002, Author retains full rights.

Appendix B

SecureScope™
by Secure Decisions,
a Division of Applied Visions Inc.

The following is an excerpt from a Power Point presentation titled "Visualization for Information Security Situational Awareness" which was posted on the Secure decisions web site (http://www.securedecisions.com/documents/SecureScopeOverview022602.ppt).[6]

© SANS Institute 2002, Author retains full rights.

Overview –

"SecureScope visually correlates data from multiple sensors in an RDBMS. SecureScope interfaces with any common RDBMS.

SecureScope Goals:

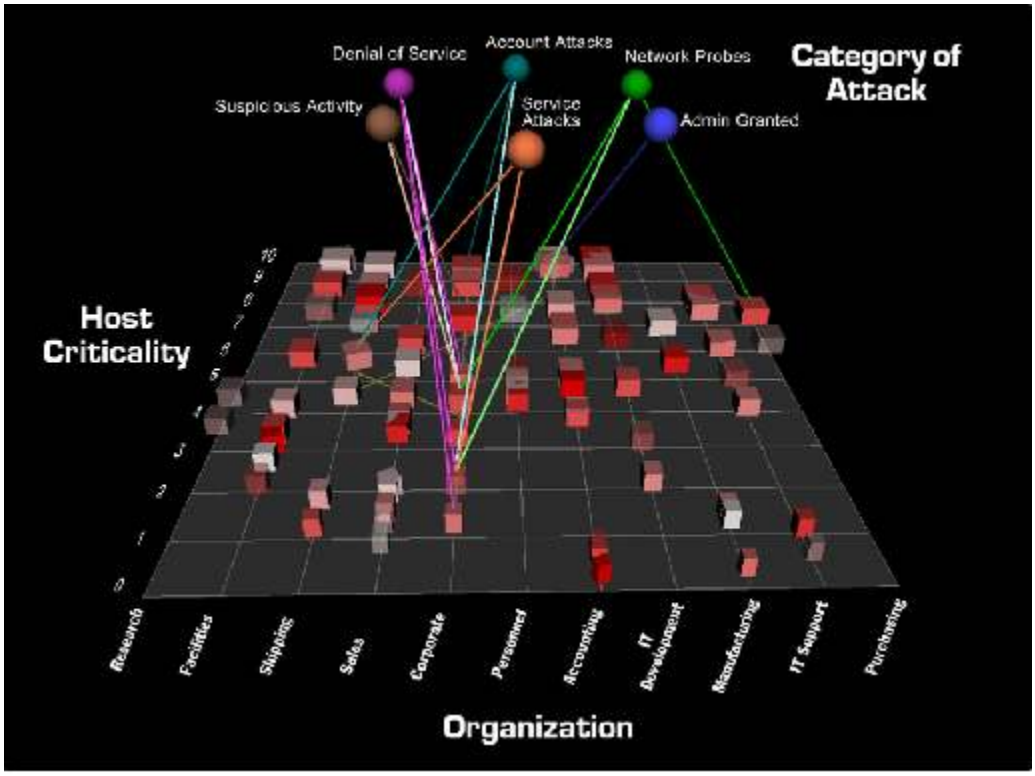
- Improve analysts situational awareness
  - Speed detection of patterns
  - Reduce mental workload
- Get more value from existing sensors (e.g. IDS, firewalls)
- Leverage people's innate ability to detect visual patterns
- Reside on an affordable platform
- Be easy to use"[6]

Summary –

"Targeted users:

- Information Security Officers and Network Administrators
- Information Security Analysts and Consultants
- Network Operations Centers and Security Monitoring Centers"[6]

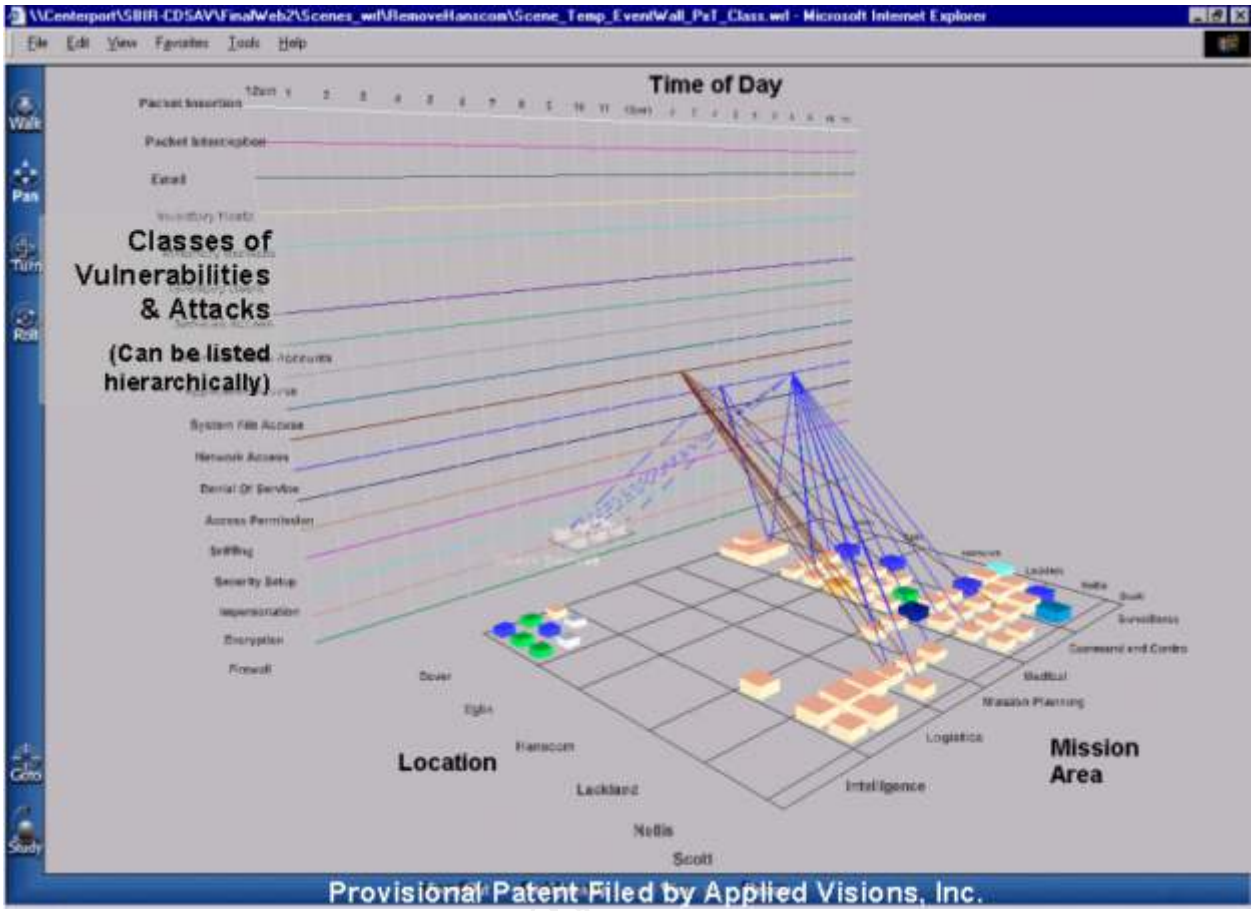
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



* 3-D visual correlation enhances discovery of patterns in security events.

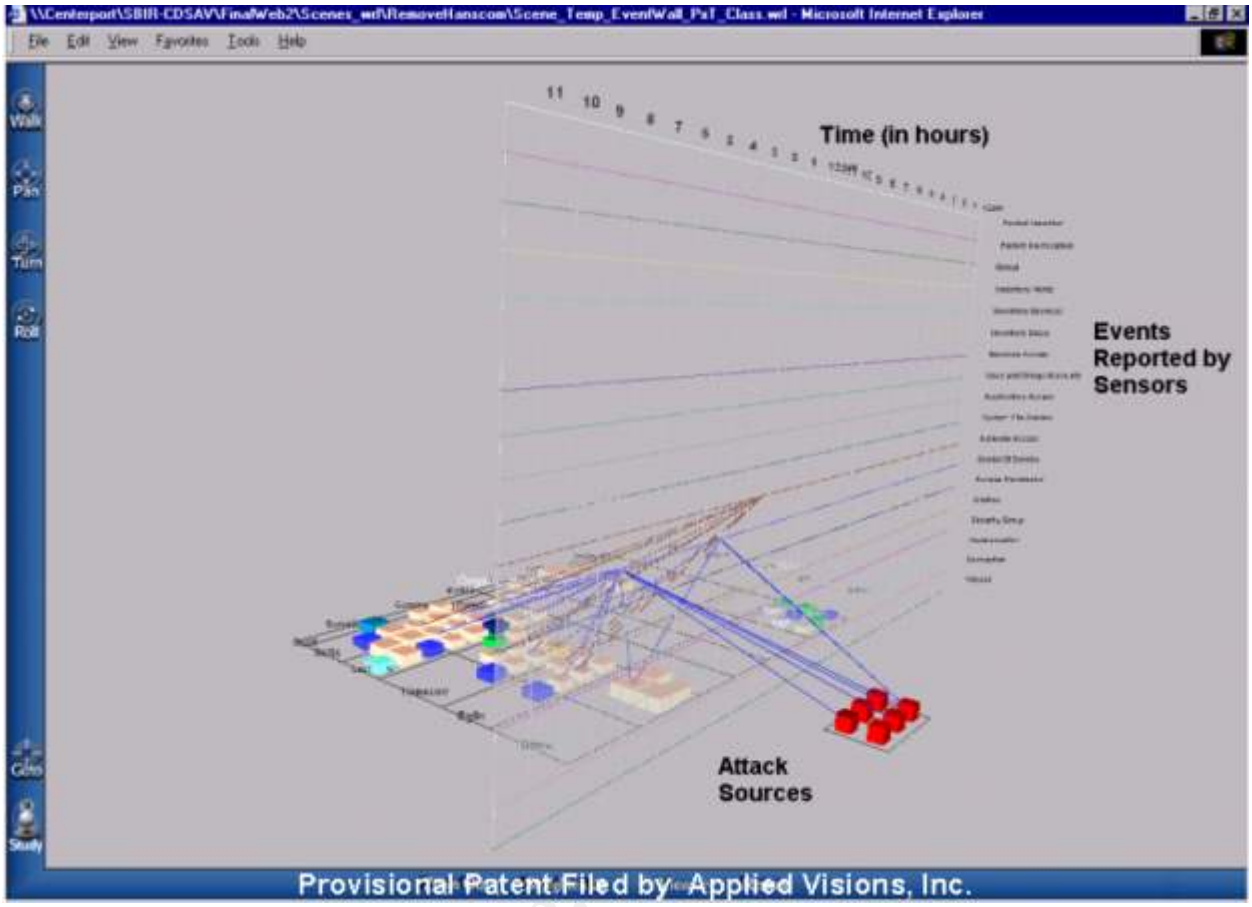
© SANS Institute 2002, Author

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



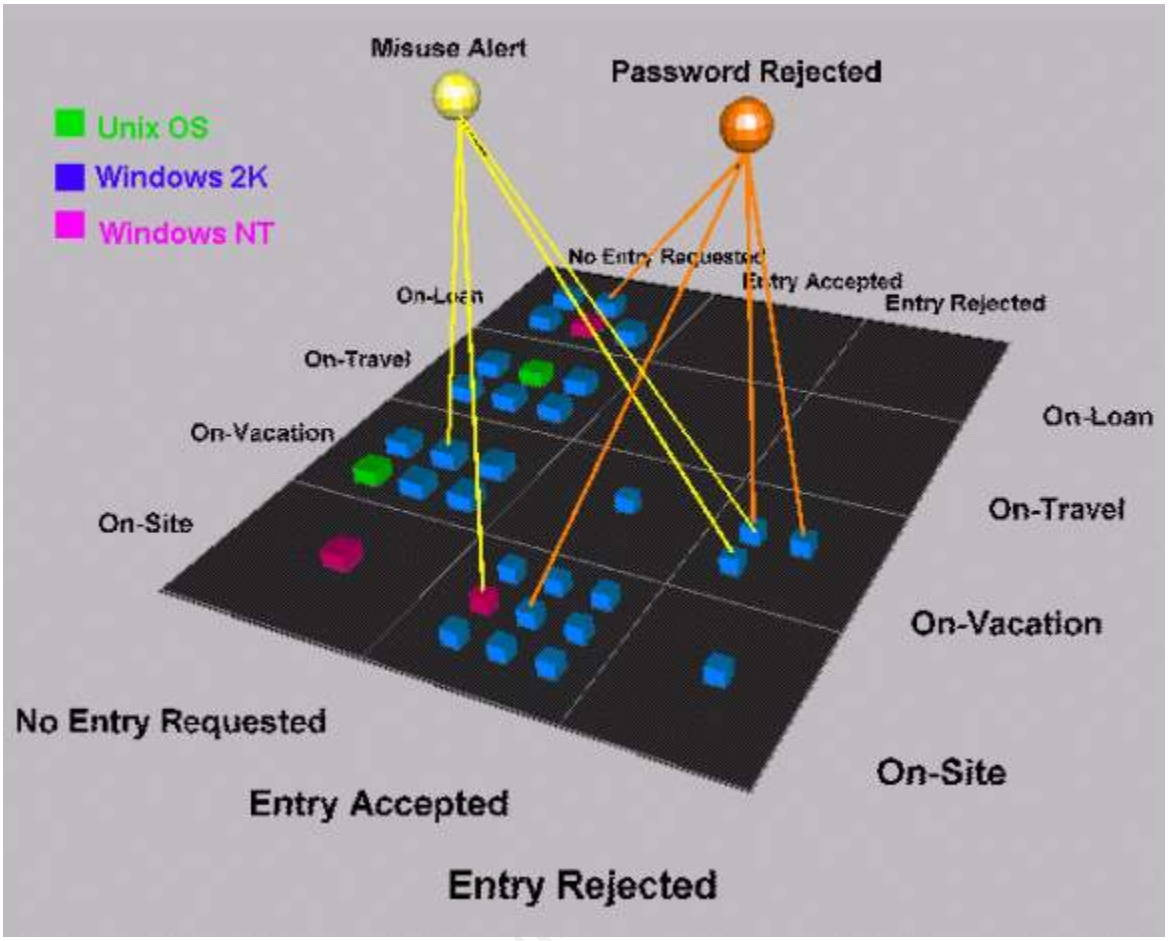
*Temporal wall links security events with the targets of those events in time.[6]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



*Rear grid can show attacker characteristics or sensor sources.[6]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



*Visualization of suspicious insider events.[6]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix C

"Open e-Security Platform"
(e-Security Incorporated)

as written by Winn Schwartau

Because I don't have personal experience with e-Security Incorporated's Open e-Security Platform, all of the following ideas and quotations are derived from a white paper titled "Solving 'Dumb Days' with Security visualization" which was written by Winn Schwartau and is posted on the Ebiz.Net web site:

http://e-serv.ebizq.net/shared/white_papers.jsp?ID=schwartau_1.pdf[7]

Note that in order to download this paper you must be a registered Ebiz.Net user with a login and password. Although I downloaded the white paper on 17 March 2002, I was unable to determine when it was actually written/published. However, the information it contains is relevant and supports the objective of this practical.

"Winn Schwartau is President of Interpact, Inc., a security awareness consulting firm, the founder of Infowar.Com (www.infowar.com), and the author of numerous books and articles about information security including "Time Based Security," and his latest, "CyberShock." He can be reached at winns@gte.net."[7]

Overview –

Mr. Schwartau suggests that the two precepts of intrusion detection in "Time-Based Security" are:

> "1. Discover that the bad guy is doing bad guy things as quickly as we can. A door alarm will detect that the seal has been broken in less than a second. We need similar approaches in information security."[7]
>
> "2. Then we have to react to the online threat immediately to mitigate the potential for damage."[7]

He supports his "Time-Based Security" theory on the premise that "Time-Based Security invites network performance and diagnostic monitors to complement other detection methods in gathering a more complete picture of the network. Monitoring tools are effective at identifying software at nodes in the network and often are used for copyright/license compliance. However, the same mechanisms are applicable for identification of miscreant software at the user's workstation." "When protection products integrate detection, the overall state of network defense will rise significantly." "Nodal Detection should be added at more nodes in a network to

© SANS Institute 2002, Author retains full rights.

improve security. Monitoring decentralized nodal system activity can provide massive amounts of information to establish norms, trends, and systemic errors when the sampling is sufficient."[7]

Thus, the same concept, when used in relation to traffic analysis, is further supported in this example: "Say a network usually operates its T-1 to the Internet at 30 percent utilization with bursts to 85 percent. Then one night, it sits at 72 percent for hours on end. If it were my company, I would like to know what the heck was going on. Wouldn't you? If Bob and Alice never talk to each other within the company network, yet over a one-week period they suddenly exchange 48 e-mails, something has changed. If John's profile says he rarely uses the Internet but he suddenly sends large amounts of data to SpiesRUs.com.cn (cn = china), as a manager I would quickly be suspicious. In all of these cases, the suspicion is raised by behavior detected through traffic analysis, not the actual contents of the communications. Traffic analysis tools make an ideal detection mechanism if the baseline profiles are reasonably set, and the reaction channel can be whatever management chooses it to be."[7]

At this point it is important to note that there are legal implications of monitoring certain types of communications, but because that is not the objective of this paper, it is only mentioned here to bring it to the attention of security professionals.[7]

Mr. Schwartau cites that the problem with collecting enormous amounts of raw data stems from the amount of time, versus the optimal time-frame for incident response that is required to process and analyze that data. The longer this process takes, the more time attackers have to do malicious things before an organization can respond. Hence, raw data alone provides little to no time relevant information, or knowledge, because it gets "stuffed in a drawer" until someone can take the time to manually analyze that data. And, "… that gargantuan task is a nightmare on the brain, the eyes, and an exercise in futility." Which brings us to the problem of "how do we handle the massive amounts of real-time data… and make decisions on what to do?"[7]

He argues that "pictures of dynamic events occurring in multiple spots across wide spans of network space are… infinitely easier than manual eye-to-brain diagnosis of network traffic patterns." And that "pictures of security-relevant events make decent network security administration feasible."[7]

The product that he is keying on is the Open e-Security Platform (OEsP) by e-Security Incorporated. "Simply, OeSP is a security management platform that performs real-time visualization of security-relevant events across an entire enterprise. In fact, their tag line is right on target: "Enterprise security you can see." There are many segmented security products which do provide visualization tools of their own small piece of the network, like perimeter intrusion detection, bandwidth utilization and firewall performance. However, OeSP integrates these functions from the leading security devices into a single view of the enterprise, depending upon what view you take."[7]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The solution that this product tries to provide to security professionals is two-fold:

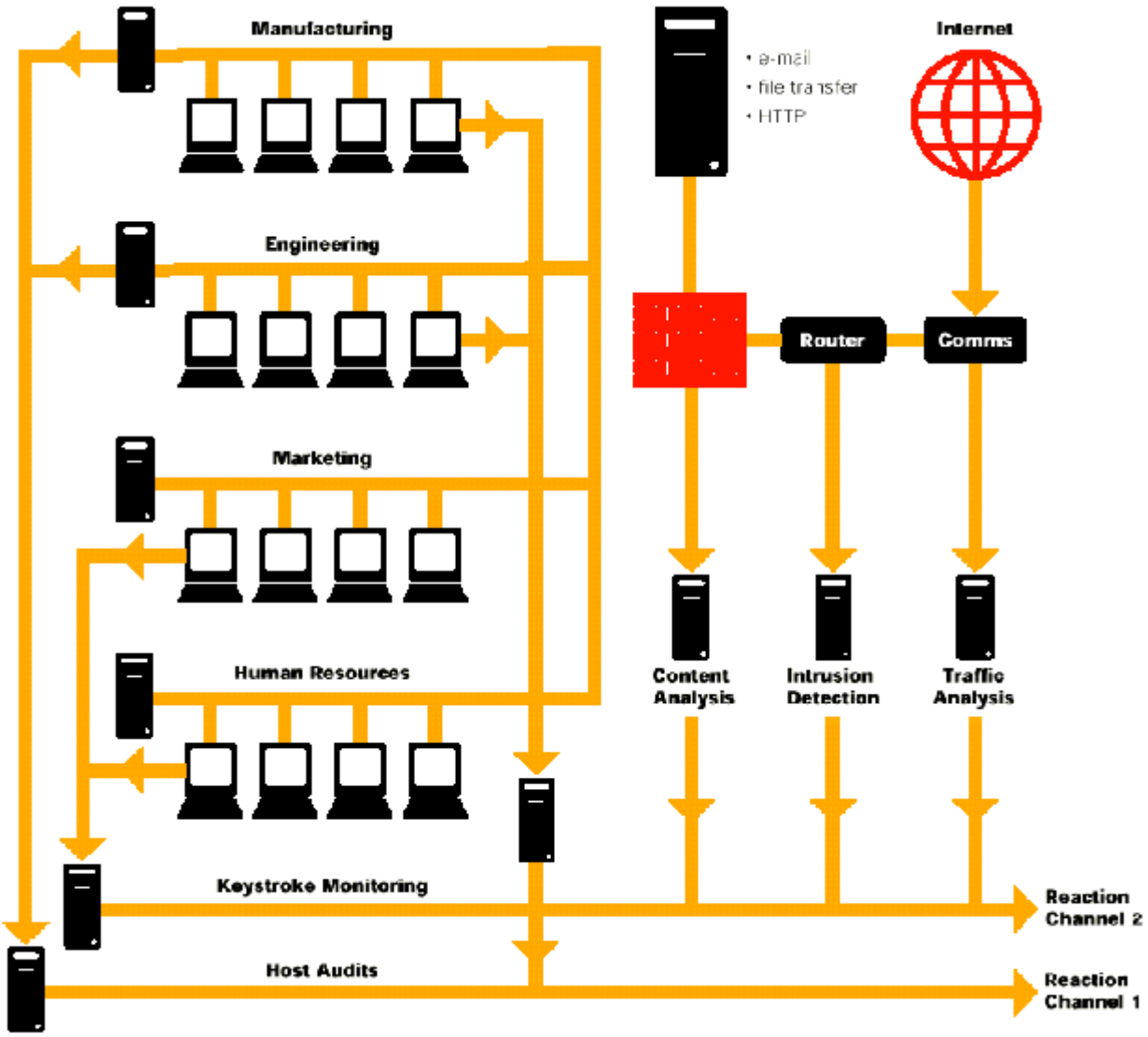
> "1. Rather than attempting to analyze several different viewpoints of the network, and then correlate them in your head or draw your own pictures and conclusions, OeSP provides a single image view of the entire network."[7]
>
> "2. You can achieve this all, in nearly real time (depending upon the speed of the host detection mechanisms), from a single console."[7]

"This way, apparently unrelated events can be correlated so that informed decisions can be made on how to react."[7]

He then provides the following example: "… in your network, does a hacker knocking at the door of your Austin, Texas-based servers have any relevance to a web-graffiti assault on your California web server? Pictures tell the story one heck of a lot easier than separate reports, separate visualization or no analysis at all. But you probably also want a more drilled-down view to understand exactly what is going on – without having to sort through a thousand pages of text or 20 different detection products. e-Security's pictorial OeSP Perimeter View of the attack now tells the administrator that the attack is coming from outside the company (the Internet) and not from the modem pool. In an eCommerce view, the entire process can be viewed in a single picture regardless of the peripheral security detection products used."[7]

© SANS Institute 2002, Author retains full rights.

Other Detection Mechanisms



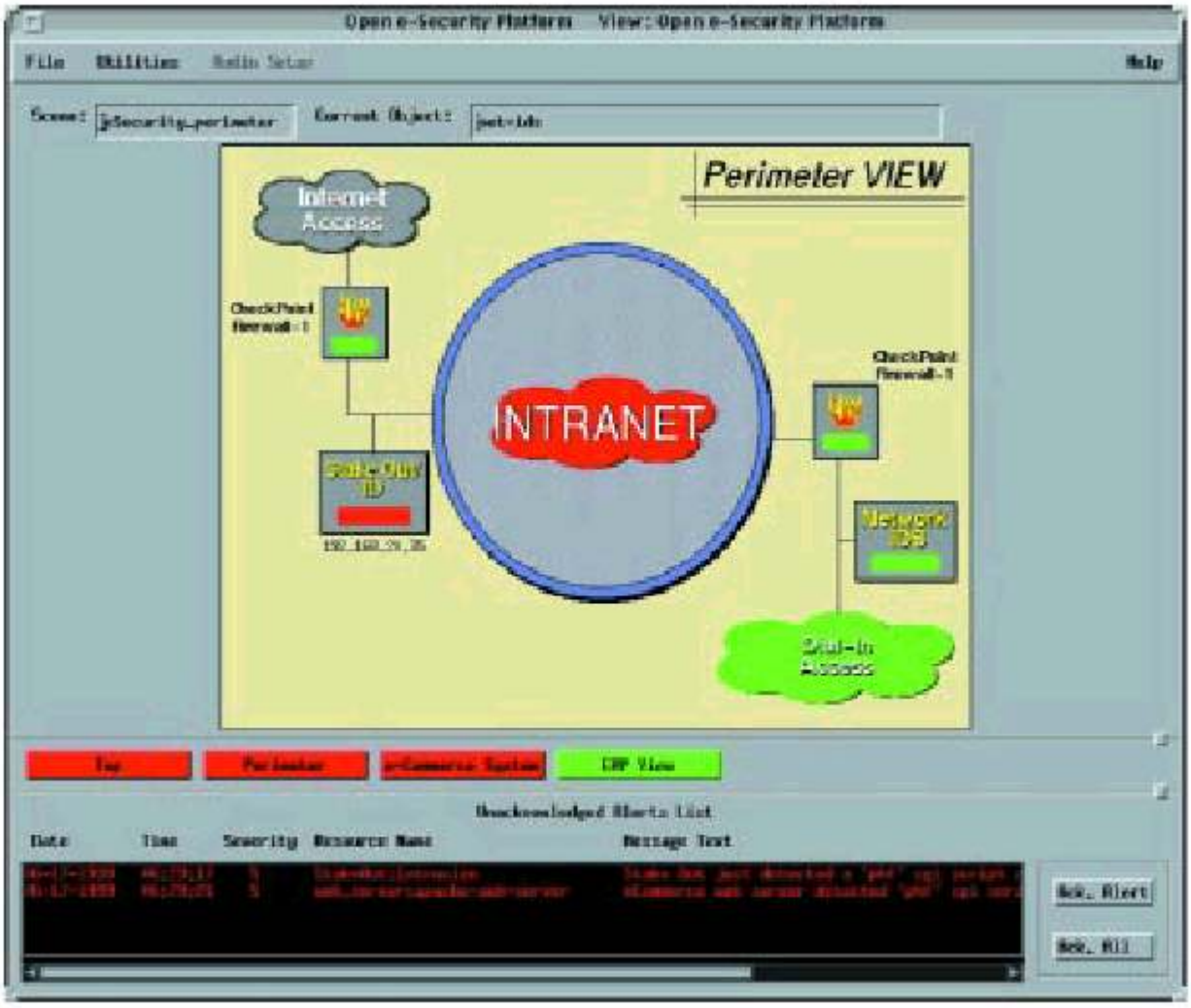
* "Detection means more than just perimeter defense, IP addresses, and hackers coming in from the Internet. Use the available data such as host audit information, traffic analysis from a NOC, and distributed IDS points throughout the enterprise network. This provides a more complete "picture" of threats to the system."[7]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Examples from the Open e-Security Platform:

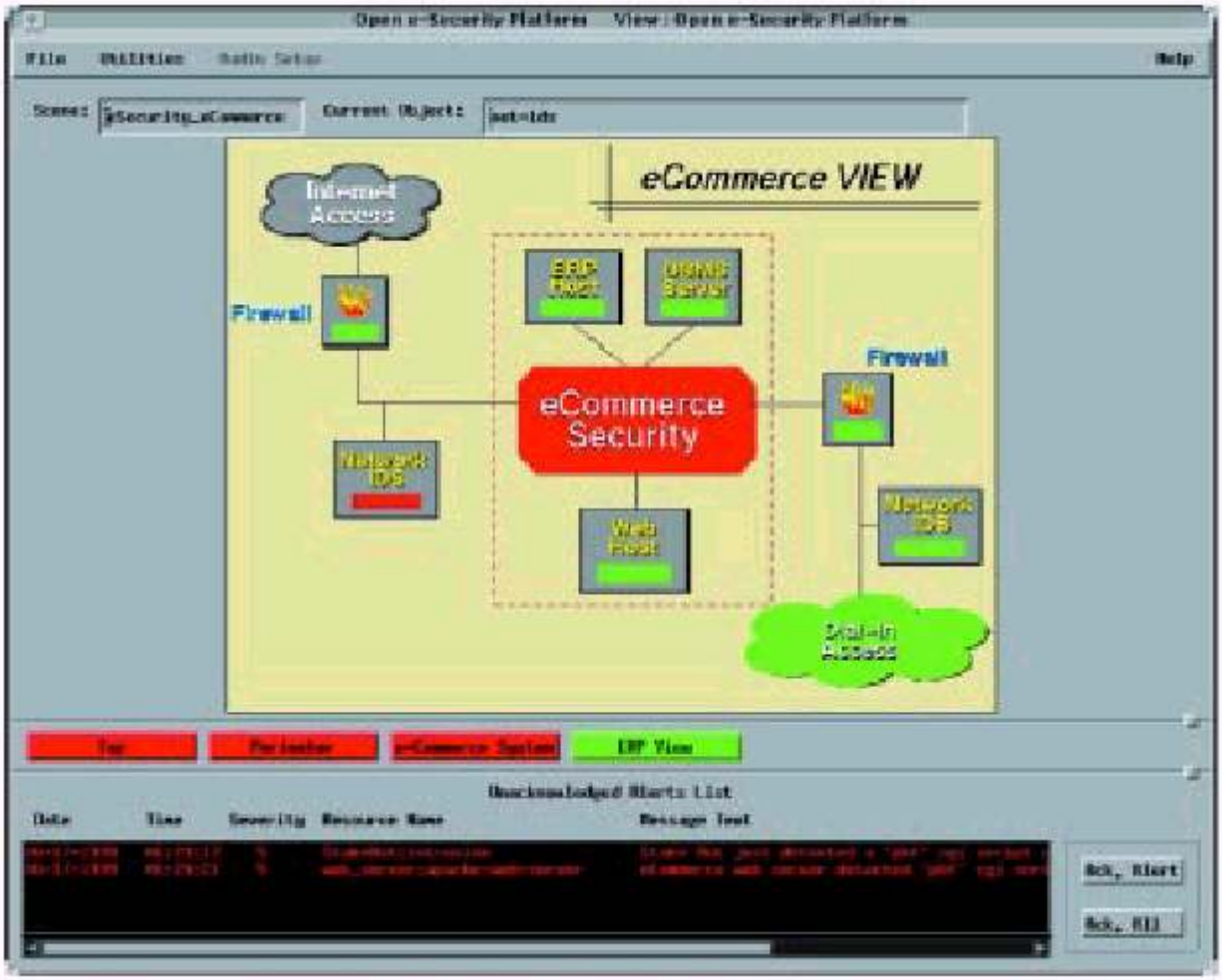
* "The Open e-Security Platform console gives you a comprehensive picture to monitor all your enterprise security resources with the flexibility to customize specific views of your security system such as e-commerce or perimeter security. Shown here is an example of a geographic view of network security across the enterprise."[7]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



* "[This] is an example of an Open e-Security Platform perimeter view of intranet security that incorporates a variety of security point security products and resources. It illustrates the console perimeter view during an attack on the network via Internet access."[7]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



* "[This] is a more detailed view of the attack within the context of the enterprise's e-commerce environment displayed in real time on the console."[7]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix D

References (Assignment 2)

[1] University of Washington. URL: http://www.washington.edu/computing/training/560/zz-tufte.html (15 March 2002).

[2] Troung, Khai N., Abowd, Gregory D., and Brotherton, Jason A. "Who, What, When, Where, How: Design Issues of Capture & Access Applications." College of Computing & GVU Center, Georgia Institute of Technology. URL: ftp://ftp.cc.gatech.edu/pub/gvu/tr/2001/01-02.pdf (20 January 2002).

[3] Green, Marc Ph.D. "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond." URL: http://www.ergogero.com/dataviz/dviz0.html. (21 January 2002).

[3a] Green, Marc Ph.D. "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond." URL: http://www.ergogero.com/dataviz/dviz1.html. (21 January 2002).

[3b] Green, Marc Ph.D. "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond." URL: http://www.ergogero.com/dataviz/dviz2.html. (21 January 2002).

[4] Eicks, Stephen G. Ph.D. "ADVIZOR™: A Technical Overview." Visual Insights, Inc. URL: http://www.visualinsights.com/pressroom/whitepapers/advisor_tech.pdf (21 January 2002).

[5] Visual Insights ADVISOR™. URL: http://www.visualinsights.com/base_pages/mainhtml.asp?level1=four&level2=three&level3=one&picked=4-1-1 (17 March 2002)

[6] Secure Decisions SecureScope™. "Visualization for Information Security Situational Awareness." Secure Decisions. URL: http://www.securedecisions.com/documents/SecureScopeOverview022602.ppt (17 March 2002).

[7] Schwartau, Winn. "Solving 'Dumb Days' With Security Visualization." Ebiz.Net. URL: http://e-serv.ebizq.net/shared/white_papers.jsp?ID=schwartau_1.pdf (17 March 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 2nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced