

**BOWIE STATE UNIVERSITY  
SCHOOL OF BUSINESS STUDIES  
ACADEMIC CENTER FOR EXCELLENCE FOR INFORMATION SECURITY**

**Program Description, Specifications and Concept of Operation**



Una Telecom, Inc. 1100  
Mercantile Lane Suite  
115A Largo, MD 20774



TransGlobal Business  
Solutions, Inc. 1100  
Mercantile Lane Suite  
115A Largo, MD 20774



Bowie State University  
14000 Jericho Park Rd  
Bowie MD 20715-9465

December 6, 2005

# Table of Content

<b>EXECUTIVE SUMMARY</b> .....	3
<b>1 BACKGROUND</b> .....	3
<b>2 OPERATIONAL ENVIRONMENT</b> .....	4
2.1 IDS/IPS LAB ENVIRONMENT .....	5
2.2 COMPUTER EMERGENCY RESPONSE AND FORENSICS LAB .....	5
<b>3 NEEDS SPECIFICATIONS</b> .....	5
3.1 HARDWARE .....	5
3.2 SOFTWARE REQUIREMENTS .....	7
3.3 SETUP AND TRAINING REQUIREMENTS .....	8
Task .....	8
3.4. COST ESTIMATES .....	8
3.5 Setup Resources .....	9
<b>4 CONCEPT OF OPERATIONS</b> .....	9
4.1 IDS/IPS SYSTEM CONCEPT .....	9
4.1.1 Architecture Summary .....	9
4.1.2 Attack Signatures .....	11
4.1.3 SiteProtector Console .....	11
4.1.4 Application Server and Sensor Controller .....	12
4.1.5 Network and Server Sensors .....	12
4.1.6. Policies and Responses .....	13
4.1.7 Event Collectors .....	14
4.1.8 Site Database .....	14
4.1.9 Security Fusion Module .....	14
4.1.10 Deployment Manager .....	14
4.1.11 Desktop Controller .....	14
4.1.12 IDS Analysts .....	14
4.1.13 Summary .....	15
4.1.14 Typical IDS Operation .....	15
4.1.15 Signature Tuning .....	16
4.1.16 System Administration .....	17
4.2 FORENSIC INVESTIGATION BUSINESS PROCESS .....	17
<b>SUMMARY</b> .....	18

## Executive Summary

On October 25, 2005 Bowie State University (BSU) along with partners Una Telecom, Inc. (UNATEK) and TransGlobal Business Systems, Inc. (TransGlobal) signed a memorandum of understanding to implement a network security laboratory. The formal agreement establishes the operating parameters for Unatec/TransGlobal to assist Bowie State University's Department of Management Information Systems to set up an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) program.

The IDS/IPS program will simulate a network system similar to contemporary enterprise or corporate network system. Several components will be attached to the system including active IDS/IPS modules; as well as forensic capabilities that will be used to delivery high-quality instructions to students and engage in several R&D activities – including mandates from local and federal institutions.

When fully operational, the program will benefit BSU in different areas including:

- Production of high quality IT security professionals and industry leaders
- Establishment of active R&D programs from **which several revenue streams** will be derived
- Establishment of partnerships with federal agencies to pursue federally-mandated IT security initiatives such as the Department of Homeland Security Bio Terrorism initiative
- Others

In this document, we present an overview of the basic program content with resource and needs specifications; and describe the basic concept of operation.

## 1 Background

The Bowie State University Center of Excellence in Information Systems Assurance Research and Education will develop new programs to conduct research and train students to protect the nation's information technology systems from cyber terrorism and security breaches on the Internet.

In the wake of 911, the importance of information security has been raised recently in our national consciousness. Through the Center of Excellence, research and educational programs will be delivered to address this need.

Also, the Center of Excellence allows Bowie State to compete with the best research groups in the country for federal grants, awards and scholarship opportunities

from federal agencies and other private sector organizations, and allows students to be part of leading-edge scientific discoveries and education.

As has been pointed out by experts in the field, With the Internet so pervasive, there has been for several years a critical shortage of professionals in the area of information assurance. The federal government has recognized that higher education is the solution to protecting the nation's information infrastructure and this center will play a key role.

The goals of the Center are to contribute to several federal initiatives including the Homeland Defense initiative by collaborating with state and federal agencies to implement educational programs in information assurance -- first at the graduate level and eventually at the undergraduate level -- and to collaborate with and help train employees of local companies involved in computer security research.

Additionally, the Center provides an excellent opportunity to partner with local companies and others across the State of Maryland to obtain joint federal funding, as well as to provide potential employees to those firms by graduating well-trained students.

The center will bring together individual researchers in the School of Business Studies who have been working independently on various aspects of information-technology assurance.

The immediate goal of the center is to add an intrusion detection and prevention, and incidence response concentration in the existing master's degree program.

The purpose of information assurance is to protect and defend information systems by ensuring confidentiality and privacy, integrity and availability of service.

As we know, the field of information assurance operates on the premise that the way to ensure information assurance is to protect systems from violations, detect them immediately when they occur and react.

To this, it is envisaged that research work at the Center will focus on developing faster, flexible and more accurate methods of doing all three.

## **2 Operational Environment**

The operational environment mimics a typical enterprise distributed network system with actively deployed IDS/IPS program and forensic capability for computer emergency response.

## 2.1 IDS/IPS Lab Environment

The lab environment will consist of 8 core PCs for different applications:

- PC1- on the inside of the trusted network (victim)
- PC2 - on the public services subnet (often referred to as a DMZ) (victim)
- PC3 - on the core internet module (traffic generator)
- PC4 – Management console
- PC5 – IDS sensor
- PC6 – Utilities/Scanners (attacker)

Other PCs will be added on a case-by-case basis.

These distinct sources and destinations of malicious traffic expose students to numerous scenarios for organizing and examining alarm data.

## 2.2 Computer Emergency Response and Forensics Lab

The in-lab will serve as the main operations center equipped with all the necessary tools to teach students how to conduct full scale and comprehensive forensic investigation of an incident. This capability exposes students to the full spectrum of Computer Emergency Response activities. Two PCs are needed at a minimum:

- PC7 – Forensic tool
- PC8 – Laptop

Other utility tools are specified below.

## 3 Needs Specifications

The needs specifications are for hardware, software and resources.

### 3.1 Hardware

The software needs are specified in Table 1 below.

**Table 1: Hardware Specification**

Item	Quantity	Description	Cost, \$	Specifications/Vendor	Uses
IDS/IPS	6	Dual Booted with Linux & MS Win2k3 Server Systems. Both systems ideally would have a very high level of processor power and memory capability with fast motherboard bus speed & Gb NICs. Audio & Video capabilities are not a high priority on			IDS/IPS

		these systems. SCSI adapters should also be included to ensure SCSI Drive analysis capability.			
Forensic Investigation Server (high-end)	1 - (The Server is for investigations using Encase, etc.)	Dual Booted with Linux & MS Win2k3 Server Systems. Both systems ideally would have a very high level of processor power and memory capability with fast motherboard bus speed & Gb NICs. Audio & Video capabilities are not a high priority on these systems. SCSI adapters should also be included to ensure SCSI Drive analysis capability.	1475	2 Dell Dimension 5150 with specified features (Including Monitors)	In-lab
1GB Flash Drives	2	Allows export of data from live systems for immediate evidence recovery scenarios.	60 x 2 =120		Traveling forensic lab
Laptop	1	Comparable hardware & software to typical laptops, dual booted with WinXP and Linux OS. To be used as main personal workstations as well as in conjunction with other travel lab equipment	NA		For both in-lab and traveling forensic lab
Adapters	2 per adapter type	-Laptop HD to Desktop IDE -PCMCIA to Network/Disk Imaging utilities -SCSI to IDE	2x50x3=300	Any	For both in-lab and traveling forensic lab
Secure External Storage Cabinet	1	Secure storage for physical evidence security. Able to lock securely and have a singular key for each custodian per cabinet.	500	Any	In-lab
IDE & SCSI Cables	N/A	Ensure the ability to use the various hardware connection types	200	Any	For both in-lab and traveling forensic lab
Disks of varying sizes	Couple of 5X 40GB 8X 80GB 2X 300GB	For storing images	1143	Maxtor	For both in-lab and traveling forensic lab
Hard Disk Write Protects	2	Ensures data on disk does not change while performing forensic investigation & imaging processes, maintaining validity in court.	500x2=1000	Logicube	For both in-lab and traveling forensic lab
Hard Disk Duplicator	1	Fast & secure bit for bit disk duplication. Reduces potential evidence corruption & loss while providing additional evidence assurance.	2500	Any	For both in-lab and traveling forensic lab
Evidence Bags	Couple of 100 count each, Large & Small	w/ Chain of Custody & Descriptive data display	130	Any	For both in-lab and traveling forensic lab
Digital Cameras	1	Photographic evidence capability, the camera(s) with macro lenses and 128mb memory card.	200	Any	For both in-lab and traveling forensic

UPS	3	One for each system, the investigative servers should not require more than the time to save work and shutdown the system.	3x60=180		lab In-lab
8 Port GB Ethernet Switch	1	Fast data transfer to & from each system	100	Any	In-lab
Furniture	1	SOC Platform			
Total Cost					

### 3.2 Software Requirements

The software needs are specified in Table 2 below.

**Table 2: Software Specification**

Item	Quantity	Vendor	Description	Cost, \$
SITE Protector	1	ISS	For IDS/IPS management	
Server Sensor	1	ISS	IDS/IPS Sensor	
Snort	1	Sourcefire	IDS/IPS Sensor	Freeware
ACID	1		For IDS/IPS management	Freeware
Scanners	Multiple	Multiple	Assorted types	Freeware
Encase	2	Guidance Software	EnCase Forensic Edition delivers advanced features for computer forensics and investigations. With an intuitive GUI and superior performance, EnCase Version 4 provides investigators with the tools to conduct large-scale and complex investigations with accuracy and efficiency; and yields completely non-invasive computer forensic investigations while allowing examiners to easily manage large volumes of computer evidence and view all relevant files, including "deleted" files, file slack and unallocated space.	2x2400=4800
Knoppix (Penguin Sleuth)	2 Bootable Linux CD containing OS & command line forensic tools		Knoppix (Penguin Sleuth) is a Linux-based Security Tool. Actually, it is a collection of hundreds if not thousands of open source security tools. It's a Live Linux Distro, which means it runs from a bootable CD in memory without changing the native operating system of the host computer. It is meant to be used by both novice and professional security personnel but is not ideal for the Linux uninitiated. <ul style="list-style-type: none"> <li>Includes The Sleuth Kit/Autopsy - the Autopsy Forensic Browser is a graphical interface to the command line digital forensic analysis tools in The Sleuth Kit. Together, The</li> </ul>	Freeware

			Sleuth Kit and Autopsy provide many of the same features as commercial digital forensics tools for the analysis of Windows and UNIX file systems (NTFS, FAT, FFS, EXT2FS, and EXT3FS).	
FIRE	2	DMZ services, Inc.	F.I.R.E. (Forensic and Incident Response Environment) is a portable bootable cdrom based distribution with the goal of providing an immediate environment to perform forensic analysis, incident response, data recovery, virus scanning and vulnerability assessment. Also provides necessary tools for live forensics/analysis on win32, sparc solaris and x86 linux hosts just by mounting the cdrom and using trusted static binaries available in /statbins.	Freeware
Linux OS	2 to 4		A version of Linux to be installed on the in lab investigation servers as well as on the laptops. The version is to yet to be determined.	Freeware
Microsoft Office 2003	2		To be installed on Investigation Servers, allows for review of MS Office related files along with organizing and preparation of data & evidence for presentation.	2x439=878
Personal Response Kits	2		CDs containing programs & applications each DCERT member has put together for their own use in order to obtain evidence or other data related to incident response. Majority is either freeware or comes with operating systems already obtained.	Freeware
Total				

### 3.3 Setup and Training Requirements

**Table 3: Setup and Training Requirements**

Task	Resource	Duration, Hrs	Rate, \$	Amount, \$
Installation, Setup and Configuration	IDS Engineer	25	80	2000
Test Configuration/ QA	IDS /QA Engineer	8	80	640
Initial Project Management	Project Manager	8	120	960
Training	Subject Matter Expert	8	140	1120
Total				4720

### 3.4. Cost Estimates

Total hardware = \$  
Software = \$  
Setup and Training Requirements = \$

**Grand Total= \$**

### **3.5 Setup Resources**

The currently available resources are in Table 4.

**Table 4:** Program Resources

<b>Designation</b>	<b>Quantity</b>	<b>Name</b>	<b>Role</b>
Director	1		Executive Oversight
Manager	1		Program Management
Coordinator	1		Program Coordination/Engineer
Engineer	1		Program Engineer

## **4 Concept of Operations**

### ***4.1 IDS/IPS System Concept***

This section presents basic intrusion detection principles, typical system architecture, and an overview of how the implemented intrusion detection system operates within the Center of Excellence.

#### **4.1.1 Architecture Summary**

The original IDS system was based a product from Internet Security Systems (ISS) Inc. called "RealSecure™." In 2002, the RealSecure product evolved into the "SiteProtector™" product.

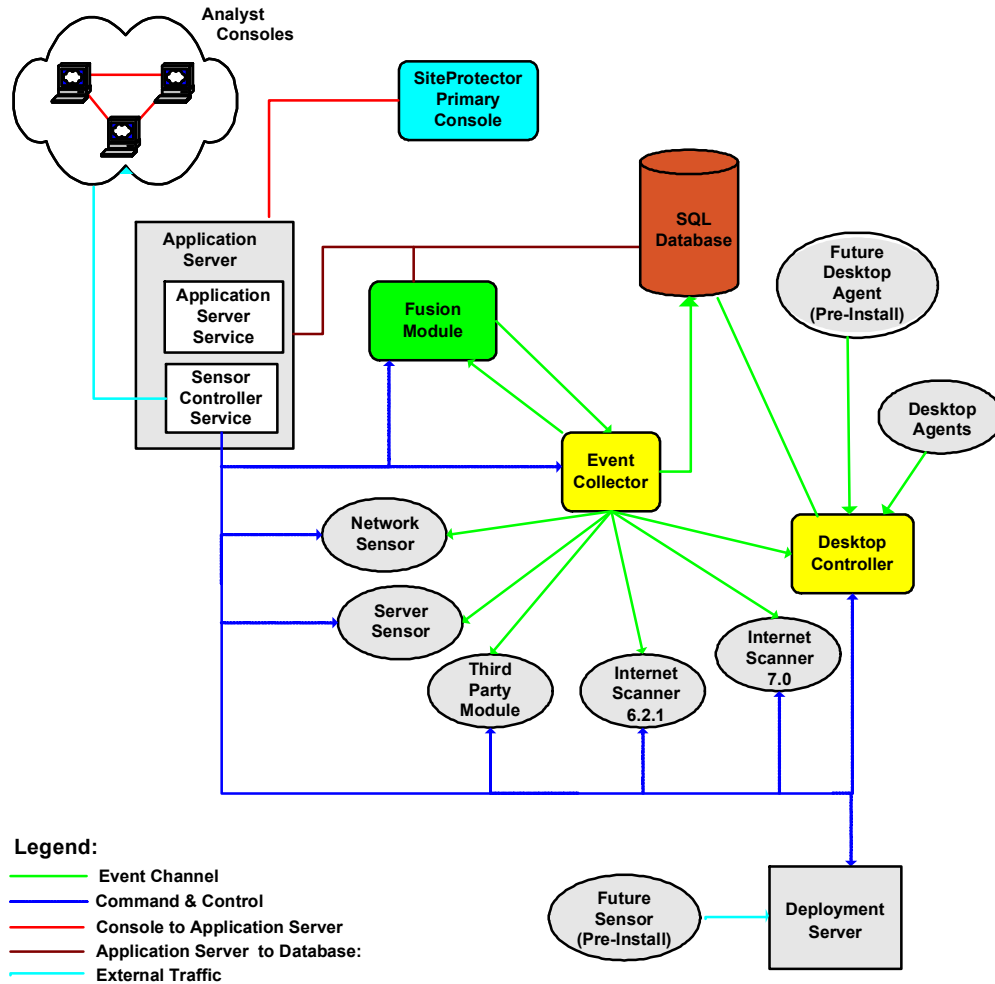


Figure 1. SiteProtector Components and Data Paths (Source ISS, Inc.).

SiteProtector components and communication paths are shown in Figure 1. The SiteProtector environment consists of one or more *Consoles* that are the control points for administering the system. One or more *Event Collectors* communicate with multiple *Network Sensors* and *Server Sensors* that are distributed throughout the network infrastructure. Sensors are placed at high-vulnerability access points throughout the network. The Event Collector performs a store and forward function – data is cached on the Collector, then forwarded to a central *SQL Database*. The Database stores event information as well as asset data for all active SiteProtector components. The *Application Server* provides communication between the Console and the Database. Sensors are configured to trigger predefined responses based upon detected attack events. The *Sensor Controller* sends commands to each sensor, i.e., commands to start or stop collecting events. A correlation engine - *Security Fusion Module* - compares detected events against known vulnerability information to determine the probability of success of the detected attack. The *Internet Scanner Databridge* places vulnerability scan data into the *SQL Database* for use by the Fusion

module. A web-based *Deployment Manager* provides for centralized software deployment and upgrade. The *Third Party Module* is an optional SiteProtector component. IDS analysts investigate intrusion events and manage the overall IDS system. Depending on the type of sensors employed, intrusion detection may be real-time or after the fact.

Attack Signatures, Consoles, Network and Server Sensors, Policies and Responses, Event Collectors, the Site Database, and analyst concepts are detailed in the following paragraphs.

### **4.1.2 Attack Signatures**

To identify potential intrusions, the system is equipped with a set of known attack signatures, also known as “decodes”. An attack signature consists of a description of data and activity type that can be recognized in a network packet stream or in a host activity log. Signatures are based on intrusion event data that are collected and analyzed by the Internet Security Systems X-Force team. Signatures are developed by ISS using a proprietary technology called Digital Fingerprinting. The collection of available signatures is referred to as a “policy.” Policies are updated by ISS on a periodic basis, typically monthly or more frequently depending on the level of activity at any point in time by the hacker community. Policies are distributed to SiteProtector customers over the Internet using a process called XPress Update (XPU).

The primary function of an intrusion detection system is to compare current data - either instantaneous network traffic or system logs - to the attack signatures. ISS RealSecure uses a combination of sophisticated protocol analysis and pattern matching to interpret network activity it detects. The success of IDS is highly dependant on the effectiveness, accuracy, reliability and the ability of the vendor to keep up with the latest attacks and newly discovered vulnerabilities. Therefore, frequent signature updates will continue throughout the life of the IDS program.

### **4.1.3 SiteProtector Console**

The SiteProtector Console provides a Graphical User Interface (GUI) to administer all of the IDS system components. It manages the network security umbrella provided by SiteProtector, including sensors and the sensor policies/attack responses. The previous generation of IDS software was built around a Master Workgroup Manager. With SiteProtector, there is no master console. Instead, multiple consoles exist, each a peer of the other. The console that is actively managing an asset holds administrative rights for that asset. Depending on network infrastructure and scalability requirements, SiteProtector components can be distributed across multiple machines, or installed in one machine. For the Center of Excellence, the SiteProtector Console, Application Server, and Sensor Controller all reside on the same machine. UNIX-based

network and server sensors are supported for the Sun Microsystems Solaris operating system. There is no UNIX platform for the SiteProtector console.

#### **4.1.4 Application Server and Sensor Controller**

The Application Server enables communication between the console and the Site Database. For the Center of Excellence IDS deployment, the Application Server shares the same server as does the Console and Sensor Controller. The Sensor Controller sends commands to the sensors, such as the command to start or stop collecting events. The Sensor Controller must reside on the same server as the Application server.

#### **4.1.5 Network and Server Sensors**

Two types of sensors are offered in the SiteProtector architecture: network sensors and server sensors, also known as Host Sensors.

The network sensor has traditionally been the workhorse of intrusion detection. These devices operate similarly to network protocol analyzers. Sensors run in promiscuous mode on the network segment (collision domain) to which they are attached, and see all network traffic traversing the segment. Sensors examine the contents of every packet on the wire while looking for attack signature matches. Typically two network interfaces are employed. One interface operates in promiscuous mode (stealth mode) so that it is not addressable or detectable by other devices. The second interface communicates over the network with the Event Collector to report suspicious events.

Network Sensors are typically deployed at Internet gateways and on network segments where there are a large number of critical resources. Since network sensors operate in real-time, it is important that they are able to process all network traffic without packet loss. *Process* in ISS terms means to capture a packet off the wire, write it to memory, examine the header, and decide whether or not the packet requires further examination. Sensors are capable of operating at Fast Ethernet and Gigabit speeds. For security reasons, information passed between the IDS sensor and its management consoles is always encrypted.

Network sensors can be software components that are installed on a UNIX or Windows 2000 host or can take the form of an “appliance” device, such as ISS’s Proventia product line. However, for supportability reasons, the Center of Excellence will use the windows 2000 Advanced Server platform for the network sensors.

Server Sensors are software modules that reside on Windows or UNIX systems. They are typically placed on mission-critical machines. Server sensors assist in situations that may be problematic for network sensors. Server sensors combine event, application, and security log analysis capabilities with a limited version of the network sensor. Server sensors see only the packets destined for the host on which they are deployed. Network speed is not the primary concern as the

server sensor sees only traffic destined for its host device. Because server sensors sit directly on the monitored host, switched networks pose no problem.

#### 4.1.6. Policies and Responses

*Policies* define the role of the sensor. Events are categorized by signature type - *Attacks* and *Audits*. Each event type is configurable. Events are then grouped by priority - High, Medium, or Low. The type of traffic seen by the sensor determines what policy is applied to the sensor.

*Attack Responses* are the acts that the sensor initiates upon detection of an attack signature match. Responses must be optimized based on the severity of the attack, yet minimize the number of false alerts. Great care must be taken in tuning of the system so that operations personnel are not subjected to excessive false alarms. The sensor policy stores the set of appropriate attack responses for each signature. Attack response options are as follows:

- Display a *Banner* message. This response is available only on server sensors. The banner response sends a message to the intruder, warning that the activity has been detected.
- *Block* the event. A range of IP addresses or network assets can be defined to allow or block network access.
- The *LogEvidence* response makes a copy of the packet that triggered an event. Evidence logs show exactly what the intruder did or attempted to do.
- *Display* lists basic information about the event on the console, in particular, event name, time, source & destination IP, sources, etc.
- The *RSkill* (RealSecure KILL) response terminates the TCP/IP socket connection. This response is not used by the IDS team.
- The *SecureLogic* response lets the analyst use Tool Command Language (TCL) scripts to respond to events and process event information.
- *LogDB* logs a summary of the event. Basic information (event name, time, source & destination IP, sources, etc.) is written to the Site Database.
- *ViewSession* allows viewing of the binary content of a session in real-time. Session data is sent to the console as it is copied off the wire.
- *E-mail* sends a notification about the event to a specified email address.
- Issue a *SNMP Trap* containing information about the event, and send it to a specified IP address that can process the SNMP information. The IDS team uses this response in with the ISM/Tivoli toolset to automate the event detection and notification process.
- The *OPSEC* response sends a message to a CheckPoint firewall, instructing the firewall to prevent the intruding source address from crossing a firewall boundary for a user-specified period of time.
- *User-specified* responses are created, as the name implies, to specify unique responses to events. Each user-specified event has a unique name and configuration. A user-specified response allows the analyst to

create a custom response by having SiteProtector open an executable file when an event is detected. This user-specified response can run any executable or batch file residing on the sensor host.

- The *Suspend* response temporarily disables the user's login account. The account is re-enabled after the specified suspend duration. Available only on Windows server sensors, and only on a few signatures.

#### **4.1.7 Event Collectors**

The Event Collector pulls data from the sensors and stores the data in the database. For the Center of Excellence the Event Collector will be installed on a stand-alone server for performance reasons.

#### **4.1.8 Site Database**

The Site Database stores events detected by network and server sensors, data from Internet Scanner (via the Databridge), data from Desktop Agents, and data forwarded from the Event Collectors. Reports can be run against this database. Communication between the Event Collector and the Site Database is encrypted. Also known as SQL Database, or Database Server.

#### **4.1.9 Security Fusion Module**

The Security Fusion Module (also known simply as Fusion) correlates data from multiple sources, including network and host sensors, and Internet Scanner in efforts to reduce the number of false positives the sensors may generate. For the Center of Excellence IDS deployment architecture, the Fusion module resides on a standalone server.

#### **4.1.10 Deployment Manager**

The Deployment Manager provides the capability to install SiteProtector components from a central computer on the network. After installing a Deployment Manager, the SiteProtector installation CD is not needed to perform an installation. For the Center of Excellence IDS architecture, the Deployment Manager will be on a stand-alone Server.

#### **4.1.11 Desktop Controller**

The Desktop Controller provides the capability to deploy and control ISS Personal Firewall agents on remote desktops. The envisaged IDS deployment will not include this component of SiteProtector.

#### **4.1.12 IDS Analysts**

The component most critical to the success of intrusion detection is the analysts. IDS analysts are technically trained personnel with strong skills in the area of network and computer security. The analysts monitor event activity, investigate both successful and failed intrusions, maintain the sensors with current attack signatures and system updates, manage the day-to-day operation of the overall IDS system, interface with security personnel, work with the Points of Contact on

all of the IDS program segments (i.e., corporate, Collaboration, etc., and participate in sustaining engineering efforts for the IDS equipment.

#### **4.1.13 Summary**

The Intrusion Detection System envisaged for the Center of Excellence includes both network based and host based sensors. Future development will ultimately add an expanded and fully integrated packaged IDS/IPS product offering.

#### **4.1.14 Typical IDS Operation**

IDS sensors – both network and server - operate 24 hours per day, 7 days a week. Automated 24x7 monitoring is provided by means of integration of IDS with the ISM toolset. IDS analysts conduct live monitoring of the IDS during normal business hours and during periods of high alert. The intrusion detection process and response procedure is detailed in the following paragraphs.

All packets traversing a monitored segment are reflected to a network sensor. Using information stored in the attack signature database and ISS proprietary protocol analysis, the sensor analyzes every packet for a possible intrusion. Packets that do not trigger an event are discarded. When an attack match is detected, data pertaining to the attack is copied to the sensor data buffer. Periodically, when the number of records on the sensor reaches a predetermined limit, the sensor uploads all of its event data to the Event Collector, and then flushes its buffer. The Event Collector forwards event data to the Site Database and to all active SiteProtector consoles. The security Fusion module compares detected events to scanning data brought in through the Databridge. Events are then correlated to determine the probability of attack success.

In addition to real-time monitoring, analysts can access the event data in the SiteProtector Database using analysis and reporting tools integrated into the SiteProtector system. In the previous RealSecure environment, much of this analysis was provided by the standalone FastAnalysis tool. As part of their day-to-day activity, analysts assess event data for suspicious activity. When intrusions are suspected or detected, the analysts work with staff to verify the validity of the attack, locate the owner of the offending machine, remove the machine from the network, or notify the appropriate BSU representative. Depending on the severity of the attack, the problem may immediately be escalated to crisis level to minimize the damage of a successful intrusion, as was the case with the MSblaster and Nachi worm infection in August 2003.

The ISS RealSecure software has the capability to automatically shut down a TCP/IP socket connection in the event of an attack. The process is called *RSKill*. Due to some limitations, the Center of Excellence will not use this feature.

#### **24x7 Operation**

The Intrusion Detection System can be monitored on a 24x7 basis, for both system health and SiteProtector attack detection. System health is monitored by

the Infrastructure Systems Management (ISM) service. At approximately five minute intervals, ISM polls the operational state of a number of hardware and software system parameters. ISM also monitors the "heartbeat" of selected sensors and SiteProtector components. ISM agents collect system health statistics via SNMP (Simple Network Management Protocol), and forward that information to a central ISM repository. When ISM detects that a system is not functioning properly, a Remedy ticket is automatically generated and sent to the appropriate Remedy queue for follow up the responsible organization.

However, it is not envisaged that monitoring will be for 24 x7 during the initial phase of the deployment.

#### **4.1.15 Signature Tuning**

When a sensor (network or server) is installed, one of a number of policies provided by the vendor is selected, applied to the sensor, and sensor monitoring is started. The policy selected is chosen based on whether it is a network or server sensor, and the type of packet traffic that will be seen by the sensor. For example, a Solaris sensor may have a UNIX-specific policy applied. A network sensor placed on a segment that is heavily used for WWW browsing may use a policy geared heavily toward monitoring HTTP vulnerabilities.

Each policy can consist of as many as 1,300 signatures. Each signature represents a different type of vulnerability. Each signature is either active or inactive by default, depending on the type of policy. In this context, *active* means that the signature is monitoring traffic real-time, and that it will trigger an alert if the packets traversing through the sensor contain data that matches the footprint stored in the signature. *Inactive* means that the signature has been turned off and that it will never trigger an alert until it is activated by one of the analysts.

As the sensor triggers alerts, analysts validate whether the alarm is normal or a false alarm. For example, if the signature detected an ftp transfer in process on a machine where there should be no ftp traffic, that event constitutes a positive alert and requires follow-up because the ftp may mean the machine has been hacked. On the other hand, if ftp is considered normal traffic in that environment, then the alert is a false alarm. The analyst would then either turn off that signature completely, add a filter to eliminate selected source/destination addresses, or modify other signature parameters to lower the response priority of that signature. This process of iteratively tuning the signatures in each policy is called baselining.

Baselining signatures are performed for every new sensor installation. The process can take as long as two weeks. It is also performed periodically on all the sensors, and whenever an updated signature file (XPress Update) is received

#### **4.1.16 System Administration**

The Information Systems department will provide backup and restoration services for all of the IDS dedicated systems, i.e., Event Collector, Database Server, Console/Application Server/Sensor Controller and Fusion.

Administration of the SiteProtector toolset is the responsibility of the IDS analysts. Detailed system administration, procedures and Standard Operating Instructions (SOI) are explained in the IDS Operations Guide document.

#### **4.2 Forensic Investigation Business Process**

Generally, the forensics business is enhanced with on-site as well as remote capabilities. The on-site capability has different systems for analysis purposes these have been described in Table 2.

But the core forensic tools used for various purposes are: Guidance Software Encase, Knoppix, AccessData FTK, Ultimate Toolkit, Smart, and a host of other small utilities (mostly Linux based).

The operational procedure/Concept of operations is based on the SANS incident handling program, which is available at:  
([https://store.sans.org/store\\_item.php?item=62](https://store.sans.org/store_item.php?item=62)).

The main goal is to uncover attacks or breaches through individuals who perform forensic analysis, incident response and intelligence gathering with deployed tools like the IDS, and the expertise required for these individuals include detailed traffic analysis and analytical skills.

The mechanics of a typical forensic investigation process are:

- Attaching subject host's disks to the investigatory system
- Mounting blank disk to store images on
- Mounting file systems with loopback device (when applicable)
- Imaging subject disk to storage file system
- Transferring images to lab machine
- Duplicating host
- Conducting investigations using any desired application package like, Encase, Sleuth kit, Coroner's kit
- Documenting results
- Preserving original and image copies

The stages with the business process activities are presented in the following Table.

**Table 5: Forensic Investigation Business Process**

Stage	Activity
<b>Arrival</b>	<ul style="list-style-type: none"> <li>• Document time of arrival</li> <li>• Photograph scene &amp; all potential evidence</li> <li>• Discuss issue with proper personnel</li> <li>• Describe the plan of action with authorized personnel</li> </ul>
<b>Investigation</b>	<ul style="list-style-type: none"> <li>• Document time of "First Touch", when the computer system is first changed in any manner (includes power off)</li> <li>• Response investigator proceeds with plan of action, determining appropriate action for this particular investigation, documenting each step taken.</li> <li>• Complete on-site investigation, document time, gather all evidence and documentation. Process and handle evidence according to procedures.</li> </ul>
<b>Administrative/Technical Management</b>	<ul style="list-style-type: none"> <li>• Open new case file, place all investigative documentation into the file.</li> <li>• If drive or data has not already been duplicated, duplicate for retention.</li> <li>• Proceed with investigation using additional tools and utilities.</li> <li>• Document each step taken.</li> <li>• Upon leaving the lab, ensure all evidence and documentation is secured and access by anyone other than the investigator is prohibited.</li> </ul>
<b>Completion and Closeout</b>	<ul style="list-style-type: none"> <li>• Ensure all documentation is gathered.</li> <li>• Ensure all evidence is consolidated</li> <li>• Determine need for retention of evidence, placing evidence in secure environment if necessary.</li> <li>• Wipe any drives with duplicate data pertaining to the investigation that is not to be retained.</li> <li>• Wipe all drives pertaining to the investigation if no data is to be retained.</li> <li>• Seal case file and store for retention.</li> </ul>

## Summary

The above-described program integrates the basic modules and components – IDS, IPS and forensics – that will become the cornerstone of the Center of Excellence.