**Version 0.2**

**38th Cyberspace Readiness Squadron**

**GENESIS OVERVIEW**

**SCOTT AIR FORCE BASE, iLLINOIS**

**DD - DD MOnth YYYY**

DO NOT RELEASE-DRAFT

Prepared by:

Title/Rank First Last

38th Cyberspace Readiness Squadron

38 CYRS/SCO

Scott Air Force Base, Illinois



Distribution C:

Distribution authorized to US

Government agencies and

their contractors; refer other

requests for this document to

[38cyrs.sco@us.af.mil](mailto:38cyrs.sco@us.af.mil)

**Document Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **POC** |
| 15-Oct-14 | 0.1 | Initial outline | Amber Carlock |
| 22-Oct-14 | 0.2 | Major updates and changes to document content | Amber Carlock |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**APPROVING/RELEASING AUTHORITY**

**SUBJECT: Genesis OVERVIEW**

**dd – dd Month YYYY**

**PREPARED BY:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FIRST M. LAST, Rank/Civ/Cntr

Position, Organization

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FIRST M. LAST, Rank/Civ/Cntr

Position, Organization

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FIRST M. LAST, Rank/Civ/Cntr

Position, Organization

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FIRST M. LAST, Rank/Civ/Cntr

Position, Organization

**APPROVED FOR RELEASE:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FIRST M. LAST, Rank/Civ/Cntr

Position, Organization

**Table of Contents**

[1. PURPOSE 1](#_Toc402172064)

[2. OVERVIEW 1](#_Toc402172065)

[3. GENESIS SYSTEM DESCRIPTION 1](#_Toc402172066)

[4. GENESIS SYSTEM COMPONENTS 2](#_Toc402172067)

[4.1. Genesis Support Servers 2](#_Toc402172068)

[4.2. Genesis Client 3](#_Toc402172069)

[4.3. Genesis User 3](#_Toc402172070)

[5. SYSTEM CAPABILITIES 3](#_Toc402172071)

[5.1. Collect Network Data 3](#_Toc402172072)

[5.2. Secure Network Data 3](#_Toc402172073)

[5.3. Terminal Licensing 4](#_Toc402172074)

[6. SOFTWARE DEVELOPMENT AND MAINTENANCE ENVIRONMENT 4](#_Toc402172075)

[7. SYSTEM CRITICALITY 4](#_Toc402172076)

[7.1. Loss of Availability 4](#_Toc402172077)

[7.2. Loss of Integrity 4](#_Toc402172078)

[7.3. Loss of Confidentiality 4](#_Toc402172079)

[7.4. Loss of Accountability 5](#_Toc402172080)

[8. CLASSIFICATION AND SENSITIVITY OF DATA PROCESSED 5](#_Toc402172081)

[9. LIFE-CYCLE OF THE SYSTEM 6](#_Toc402172082)

[9.1. Design 6](#_Toc402172083)

[9.2. Construction 6](#_Toc402172084)

[9.3. Operation 6](#_Toc402172085)

[9.4. Termination 6](#_Toc402172086)

[10. SYSTEM SECURITY FUNCTIONS 7](#_Toc402172087)

[10.1. Internet Protocol Security (IPSec) 7](#_Toc402172088)

[10.2. Login Security 7](#_Toc402172089)

[10.3. Audit Logs 7](#_Toc402172090)

[10.4. Virus Protection 7](#_Toc402172091)

[11. SYSTEM USER DESCRIPTION AND CLEARANCE LEVELS 8](#_Toc402172092)

[11.1. Users 8](#_Toc402172093)

[11.1.1. Primary Users 8](#_Toc402172094)

[11.1.2. Base/NOSC Network Administrators 8](#_Toc402172095)

[11.1.3. Foreign National Users 8](#_Toc402172096)

[12. SYSTEM SECURITY ROLES/RESPONSIBILITIES 8](#_Toc402172097)

[12.1. Program Manager (PM) 8](#_Toc402172098)

[12.2. Information Assurance Managers (IAM) 9](#_Toc402172099)

[12.3. System Administrator (SA) 9](#_Toc402172100)

[12.4. Users 9](#_Toc402172101)

[13. Appendix A: Acronyms and Definitions 10](#_Toc402172102)

[14. Appendix C: Definitions 11](#_Toc402172103)

[15. Appendix B: Cyber Security Engineering 12](#_Toc402172104)

[16. Appendix C: Cyber Systems Engineering 13](#_Toc402172105)

[17. Appendix D: Cyber Network Engineering 20](#_Toc402172106)

**TABLE OF FIGURES**

[Figure 1: Genesis v3 System Overview 2](#_Toc402172107)

[Figure 2: SCOPE Genesis Processed Data 6](#_Toc402172108)

[Figure 3: Data Classification Level Comparison 6](#_Toc402172109)

1. PURPOSE

The purpose of this document is to provide an overview and description of the capabilities, responsibilities, and functions that apply to the operation of SCOPE Genesis.

1. OVERVIEW

The SCOPE Genesis system is a software platform and suite of tools used by qualified network and systems engineers to remotely gather and analyze network configuration and performance data. The use of this system automates and expedites numerous tedious and time-consuming tasks required to develop a complete picture of a network’s current state. When deployed to a site in advance of an on-site visit, Genesis is accessible via Internet Protocol Security (IPSec) which provides superior, encrypted end-to-end security.

1. GENESIS SYSTEM DESCRIPTION

The SCOPE Genesis system is designed to provide a means to remotely and securely survey a base network.

Figure 1 shows the components of the Genesis system. The system consists of:

1. *Genesis Client* (deployed operating system)
2. Terminal Services/Licensing Server
3. Remote workstations
4. Backup server

Additional support services:

1. Microsoft Windows Software Update Server (WSUS)? for patch management
2. Windows Deployment Server for system image management
3. Symantec Antivirus Server

The *Genesis Client* is installed at the remote location (Integrated Network Operations and Security Center (I-NOSC)/Base Network Control Center (NCC)) prior to an on-site visit. Qualified network and systems engineers connect to the *Genesis Client* from their assigned workstation through an IPSec tunnel using Terminal Services. The engineers then execute various applications and scripts on the *Genesis Client* to collect network configuration data from the remote Major Command (MAJCOM) /base NOSC/NCC network. Prior to remote data gathering, technicians at the base or facility where the Genesis was sent must provide accounts with administrator level access to the network that is to be assessed. A home station file server is used as a data repository for data collected from each base surveyed. A backup server provides disaster recovery services, and a Terminal Services License Server provides license tracking services for deployed laptops.

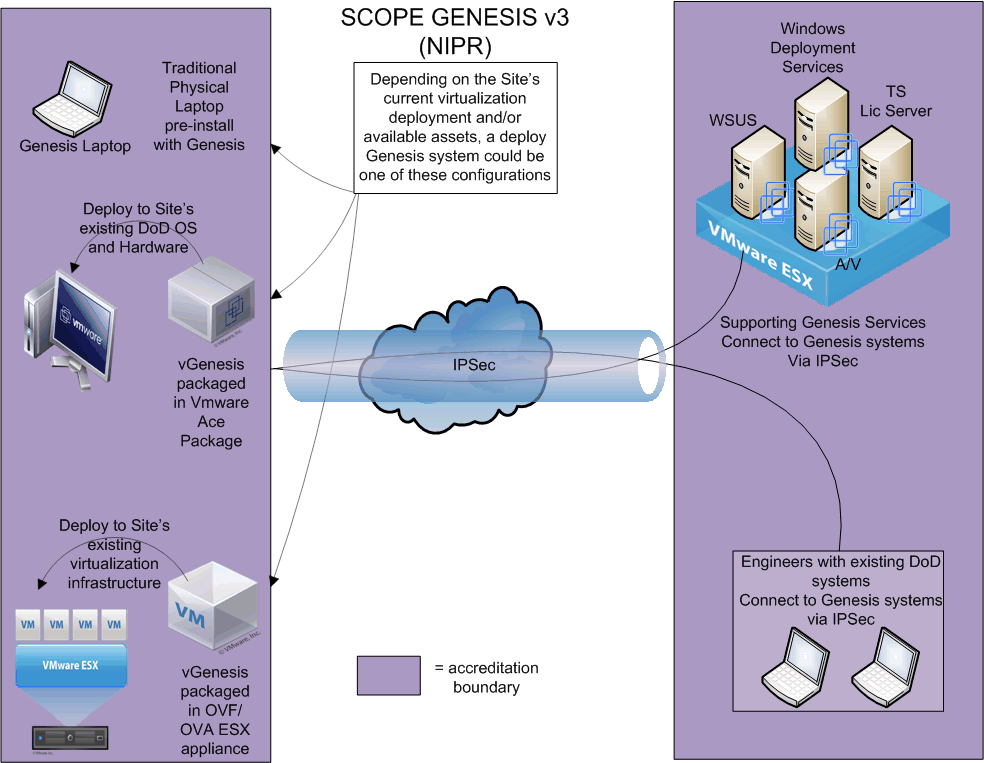
****

Figure 1: Genesis v3 System Overview

1. GENESIS SYSTEM COMPONENTS

Genesis functionality is broken down into 3 discrete elements all of which must function together to provide the capabilities Genesis is capable of accomplishing.

* 1. Genesis Support Servers

All Genesis system hardware is maintained by qualified technicians and coordinated by a Configuration Control Board (CCB). The Genesis Support Servers provide the management and administration features utilized by the network and systems engineers and the Genesis client platforms. These services include:

* Server 1 - Core Services: Administration, licensing, file sharing
* Server 2 - Security services: Patching/AV/Scanning
* Server 3 - Backup and Deployment: WDS/Imaging
* Server 4 - Database: Trending/Analysis and SQL/SharePoint Databases
  1. Genesis Client

Genesis clients consist of the discovery, collection and analysis platform utilized during the network assessments. These clients may be deployed through 3 methods:

* Physical Laptop
* Virtual Machine on standard hardware in VMWare ACE package
* Virtual Machine to VMWare virtualization suite in ESX appliance
  1. Genesis User

Genesis users consist of qualified network and systems engineers equipped with laptops configured with the Air Force Standard Desktop Configuration (SDC) and standard network assessment toolset.

1. SYSTEM CAPABILITIES

Genesis and the suite of tools that accompany it provide two primary capabilities: Network Optimization and Network Configuration Standardization and Evaluation (Stan/Eval). SCOPE Genesis increases the efficiency of on-site visits by decreasing the time needed to understand and assess the network at the deployed location. For some assessment efforts, the Stan/Eval assessment can be done remotely through the Genesis system. The SCOPE Genesis system’s primary capability is to collect data on a remote network. By providing remote analysis capability, SCOPE Genesis allows on-site team more time to explore issues that can’t be resolved remotely, engineer solutions that require on-site analysis, and work with local network administrators on implementing recommendations for securing and optimizing their networks.

* 1. Collect Network Data

The main capability of the Genesis system is to provide a secure conduit and suite of tools through which qualified network and systems engineers can survey a base network and collect data on types and locations of network devices, device configurations, and data that provides insight regarding network performance. The network survey is initiated by qualified network and systems engineers using workstations which are remotely connected to the deployed Genesis laptop computer. With proper accounts and permissions established, the deployed Genesis laptop computer allows engineers to map the network, interact with network servers and workstations, interact with firewalls, interact with routers and switches, and evaluate network performance.

* 1. Secure Network Data

Due to the sensitive nature of the data gathered, it is not be acceptable to allow unprotected data communications between the remote workstations and the deployed Genesis system. SCOPE Genesis relies on IPSec as a primary means to encrypt data between the workstation and the Genesis laptop. When utilized to conduct assessments at Air Force installations; it utilizes the Air Force Virtual Private Network (VPN) as a secondary means of data encryption.

* 1. Terminal Licensing

The deployed Genesis laptop will have Terminal Services installed and hosts the connections from the remote workstations. The home station based Terminal Server Licensing Server will issue the Client Access Licenses (CALs) that are required for these connections.

1. SOFTWARE DEVELOPMENT AND MAINTENANCE ENVIRONMENT

While a few scripts and applications were developed in-house, the majority of the Scope Genesis applications and tools consist of commercial products. Accordingly, the documentation for the commercial products is provided when the software is purchased. There is a limited software development effort with milestones and cost accounting for life cycle replacement of hardware and software upgrades.

The CPT Maintenance function is responsible for configuration management and tracking future enhancements to the system. The version that is evaluated for this certification is SCOPE Genesis, version 2.0. This is an upgrade from version 1.0, which was certified and accredited in 2002. Any modifications to the system will need to be approved by the CPT Maintenance management chain, acting as an informal CCB. If it is determined that the changes represent a major modification to the system by the Certifying Authority (CA), the documents will be resubmitted to the Designated Approving Authority (DAA) and Headquarters (HQ) Air Force Communications Agency (AFCA) to update the system’s Net-worthiness certification.

1. SYSTEM CRITICALITY

SCOPE Genesis is a “mission-impaired” system. Genesis is a tool that qualified network and systems engineers use to assess Air Force networks. It provides the means to reduce costs while not degrading the assessment and analysis services provided. The Genesis system is essential in meeting all of the deployment needs to accomplish the mission. Significant portions of network discovery and analysis is accomplished through the remote Genesis laptop(s). SCOPE Genesis improves the effectiveness of on-site team visits allowing for analysis of remote network data prior to MAJCOM/Base visits. The loss of these functions would have a direct mission impact by degrading the ability to remotely capture and analyze network data.

* 1. Loss of Availability

SCOPE Genesis is designed to provide qualified network and systems engineers increased capability and make their on-site visits shorter, less costly and more efficient. If SCOPE Genesis is unavailable, engineers will be forced to fall back on contingency operating procedures, which would require lengthier, more costly on-site visits to complete assessments.

* 1. Loss of Integrity

Loss of system integrity is a concern due to the amount of access Genesis is capable of providing to base network devices. The threat to base network operations would be high if Genesis was found to have its integrity compromised, so the Genesis system relies on the network security of the base and strictly administered policies on the Genesis system itself.

* 1. Loss of Confidentiality

Genesis collects sensitive information on the status and configuration of bases networks. This information could be helpful to an adversary, person or group seeking to disrupt base network operations.

* 1. Loss of Accountability

With the level of access Genesis provides to network devices, accountability is important to the system’s operations. Again, the threat is to the base network operations and all of its associated dependencies.

1. CLASSIFICATION AND SENSITIVITY OF DATA PROCESSED

Table 2 characterizes the information processed by the SCOPE Genesis system. It is possible that Genesis will process configuration information on network devices critical to military command and control operations or the operation of a major weapon system.

|  |  |  |
| --- | --- | --- |
| **Data Type** | **Sensitivity/Definition** | **Info Processed and/or Maintained on System** |
|  | ***Classified Information*** |  |
| **National Security Information** | Data processed are CONFIDENTIAL, SECRET, TOP SECRET. Process control systems where alteration could result in a catastrophic occurrence |  |
|  | ***Sensitive Information*** |  |
| **Financial Sensitive** | Data processed are used in direct payment operations. Data compromise or alteration could result in significant legal and financial liability. |  |
| **Critical Operations** | Alteration or compromise of data contained in or processed by an application could have significant adverse effects on an agency's ability to complete its mission in an effective manner |  |
| **Personnel** | Data stored/processed are covered by the Privacy Act. Data compromise could result in legal liability but not significant financial liability |  |
| **Administrative** | Data compromise might cause embarrassment but would not result in legal/financial liability. | X |
| **Proprietary** | Information provided by non-government sources on the condition that it not be released to other non-government sources. |  |
| **Trusted Information** | Information that when received is accepted as authentic | X |
| **Security Control** | Data associated with the security mechanisms | X |
| **Source Selection Sensitive** | Information on upcoming contracts and proposals |  |
| **Logistics Information** | Data concerning the status and allocation of personnel and material to/from various locations |  |
| **Weapons system acquisition information** | Information critical to the development, deployment and/or life cycle status of a weapon system and/or support equipment |  |
| **National Security Information** | Data processed involving intelligence activities, cryptographic activities related to national security, command & control of military forces, equipment integral to a weapon or weapon system, or data which is critical to direct fulfillment of military or intelligence missions. | X |
|  | ***Unclassified Information*** |  |
| **Non-sensitive** | Small programs, easily reconstructed. No effect on agency operations if data are lost or compromised. No financial liability | X |

Figure 2: SCOPE Genesis Processed Data

Table 3 documents the relationship between the data classification levels and categories. The percentages identified account for 100% of the information processed by Genesis. While the majority of data processed by Genesis is unclassified, the aggregation of data will be rated sensitive, For Official Use Only.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sensitivity** | **Categories** | | | | | | | |
|  | **Privacy Act** | **PROPIN** | **FOUO** | **SCI** | **SAR** | **SAP** | **None** | **Etc.** |
| TS | N/A | 0% | N/A | 0% | 0% | 0% | 0% | … |
| SECRET | N/A | 0% | N/A | 0% | 0% | 0% | 0% | … |
| Confidential | N/A | 0% | N/A | N/A | 0% | 0% | 0% | … |
| Sensitive | 0% | 0% | 40% | N/A | N/A | N/A | N/A | … |
| Unclassified | N/A | N/A | N/A | N/A | N/A | N/A | 60% | … |

Figure 3: Data Classification Level Comparison

The system criticality based on the highest classification maintained and/or processed by the system would be considered: **FOUO - Dedicated (Criteria 2 system) - National Security Information (operational at certification level 2)**.

1. LIFE-CYCLE OF THE SYSTEM
   1. Design

SCOPE Genesis version 2.0 has been upgraded from its initial version, which was certified and accredited in 2002. While Genesis is expected to be continually enhanced, the design for this version is set.

* 1. Construction

Construction of version 2.0 is set, pending review of system from AF net-worthiness process.

* 1. Operation

Waiting for completion of system construction and system recertification. The initial version of SCOPE Genesis is currently operational. Expect SCOPE Genesis version 2.0 to be operational by Summer of 2005.

* 1. Termination

Termination date not yet planned.

1. SYSTEM SECURITY FUNCTIONS

Several system security functions have been utilized within the Genesis system to protect the method of communication from the Genesis User to the Genesis Client, the system itself, and the information that is gathered by the Genesis system. Employing several of these methods in a non-intrusive multilateral method allows the user of the system to focus on the collection of data.

* 1. Internet Protocol Security (IPSec)

IPSec aids the Genesis system by providing an encrypted communication method between the Genesis User and the Genesis Client. This encryption is implemented at the IP transport level, or Network Layer 3, of the Open System Interconnection (OSI) network model. This low level implementation of encryption enables a high level of protection transparently for applications, services, and upper layer protocols. This allows security measures to be transparent to the user once the encryption tunnel has been established. IPSEC connectivity is not supported or implemented on the Secure Internet Protocol Router (SIPRNET) version of the SCOPE Genesis deployed client

* 1. Login Security

Password authentication is used to verify the user’s credentials prior to allowing access to Genesis components. A Genesis user must authenticate to both the Genesis User system and the Genesis Client to be granted access to data residing on the Genesis Client.

* 1. Audit Logs

Audit logs are enabled on the Genesis Client and Support Servers as a method of tracking the activities of personnel who are accessing or attempting to access the system. These logs provide a detailed timeline of who was granted or denied access to the system. Only administrators are granted rights to examine the audit logs of Genesis Systems. Audit logs are maintained for a minimum of one year.

* 1. Virus Protection

The Genesis system will utilize the McAfee Host-based Security System (HBSS) Antivirus (AV) Client on all system components. The AV client runs constantly as a service and will provide real-time virus protection, checking each file as it is accessed or moved through the system for any known viruses. The HBSS Antivirus Client keeps a database of “Virus Definitions”. This database provides the client with the information to identify viruses. This database is updated via an “automatedUpdate” feature that contacts a locally maintained server, downloads the updated “definition files”, and installs them into the client. These “Definition Files” are updated before Genesis is installed at a remote location. If a virus is detected, it will notify the user, create a log entry in the application, and attempt to clean the file so the system may access it. If the file is unable to be cleaned, the system will quarantine the file and disallow access to it. This security measure operates with little impact on system resources, and with almost no intervention from the user of the system.

Automated update is not yet supported in the SIPRNET version of the SCOPE Genesis deployed client.

1. SYSTEM USER DESCRIPTION AND CLEARANCE LEVELS
   1. Users
      1. Primary Users

Qualified network and systems engineers will be the primary users of SCOPE Genesis. These users may be comprised of both government and contractor personnel with a SECRET level clearance. Each member with access to the system will have full access to the system’s capabilities. Currently there are three types of engineers that utilize the SCOPE Genesis to fulfill a particular function during each assessment.

* + - 1. Cyber Security Engineering (CSEC)
      2. Cyber Systems Engineering (CSYS)
      3. Cyber Network Engineering (CNET)
    1. Base/NOSC Network Administrators

The local base/NOSC network administrators will have access to the deployed Genesis laptop computers. In some cases, we will require and request their assistance in installing the laptop computer on their network. This may require local on-site administrators to access the laptop computer in order to complete installation. At that time, there should be no data processing. The local network administrators will have a valid need to know for any data processed by the laptop computers. The deployed laptop will exist within the base/NOSC network administration facility.

* + 1. Foreign National Users

The DAA has not sought foreign disclosure approval for Genesis. Should a MAJCOM request foreign disclosure approval to provide foreign national access as provided for in AFI 33-202, *Computer Security*, HQ AFCA will provide the information as requested. Foreign nationals will require the same authorization as United States of America citizen users to access Genesis, to include an existing approval to access the Non-Secure Internet Protocol Router (NIPRNET) and a letter from a U.S. Government Department of Defense security official validating the user’s clearances.

1. SYSTEM SECURITY ROLES/RESPONSIBILITIES
   1. Program Manager (PM)

The PM will implement DoD Information Assurance Certification and Accreditation Process (DIACAP) for the Genesis information system. The PM will ensure that each assigned Department of Defense (DoD) information system has a designated Information Assurance Manager (IAM) with the support, authority and resources to satisfy the responsibilities established in DoDI 8500.2. The Program Manager (PM) will plan and budget for Information Assurance (IA) Controls implementation, validation and sustainment throughout the system life cycle, to include timely and effective configuration and vulnerability management.

* 1. Information Assurance Managers (IAM)

The IAM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture as well as conducting annual security reviews of all IA controls and a test of selected IA controls.

* 1. System Administrator (SA)

SAs assist in directing the daily operations of security programs for local and remote terminal areas that are used to gain access to network equipment, applications, and various other network resources. SAs are most effective by ensuring established security policies and procedures are followed by their local workgroup. Security vulnerabilities, incidents, and problems are to be immediately reported to the SA.

* 1. Users

Computer and network security is best approached as a fundamental system component that enhances the operational environment by directly employing and relying on the system’s security functions, rather than the individual user to maintain and manage system security. One of the design goals of the Genesis System is to ensure the implemented security mechanisms are viewed as allies, rather than adversaries by the individuals who use these tools to accomplish their mission. Users are required to follow local and AF guidance on appropriate use of government computer systems. Users will report any suspected violations of the Genesis security policy, or any evidence of tampering of the system from inside or outside the user community.

1. Appendix A: Acronyms and Definitions

|  |  |
| --- | --- |
| **Acronym** |  |
| AFCA | Air Force Communications Agency |
| AFNIC | Air Force Network Integration Center |
| AV | Antivirus |
| CA | Certificate Authority |
| CAL | Client Access License |
| CCB | Configuration Control Board |
| CPT | Cyber Protection Team |
| CyRA | Cyber Readiness Assessment |
| DAA | Designating Approving Authority |
| DIACAP | DoD Information Assurance Certification and Accreditation Process |
| DoD | Department of Defense |
| GPO | Group Policy Object |
| HBSS | Host-Based Security System |
| HQ | Headquarters |
| IA | Information Assurance |
| IAM | Information Assurance Manager |
| I-NOSC | Integrated Network Operations and Security Center |
| IPSec | Internet Protocol Security |
| MAJCOM | Major Command |
| NCC | Network Control Center |
| NIPR | Non-Secure Internet Protocol Router |
| OSI | Open System Interconnection |
| OVA | Open Virtual Appliance |
| OVF | Open Virtual Format |
| PM | Program Manager |
| SA | System Administrator |
| SDC | Standard Desktop Configuration |
| SIPRNET | Secure Internet Protocol Router |
| Stan/Eval | Standardization and Evaluation |
| TS LIC | Terminal Services Licensing |
| VPN | Virtual Private Network |
| WSUS | Windows Server Update Services |

1. Appendix C: Definitions
2. Appendix B: Cyber Security Engineering

|  |  |  |
| --- | --- | --- |
|  | | |
| **Type** | **Area** | **Description** |
| Discovery | Host Enumeration | * Scanning base’s network space to determine hosts * Identifying which machines should be scanned and determining the most appropriate scan type for that machine   + Ping sweeps   + SNMP sweeps   + Port scans   + Vulnerability scans |
| Vulnerability Scanning | * Identifying specific ports open associated with services   + e.g. Port 22 open -> SSH open * Identifying default credentials in use   + e.g. username: admin & password: admin on a base HP LaserJet printer * Identifying vulnerable applications   + e.g. Adobe Acrobat Reader 9.0.0 * Identifying vulnerable operating systems/missing patches   + e.g. Missing Windows Service Pack 1 |
| Log Retrieval | * Examining HBSS logs to determine past alerts |
| Firewall Configuration Examination | * Retrieving configurations from firewalls |
| Proxy Configuration Examination | * Retrieving configurations from bluecoat proxys |
| Reports | Vulnerability Analysis | * Providing a report on devices with current vulnerabilities including a listing of vulnerable files and devices * Providing a report on devices with excess ports open or default credentials |
| Software | * Listing applications on various devices for further investigation * Listing machines with particular HBSS issues in the past for more investigation |
| Firewalls | * Reporting differences between firewalls |
| Proxy Servers | * Reporting differences between proxy servers |
| Training | Personnel | * Training on each of the processes and determining what is capable at the base or NOS level to do each of these processes * Adapting teaching methods to various levels of experience, from beginners through experts.   + e.g. Experienced folks may lose interest at low-level training   + e.g. New folks may be overwhelmed with high-level training |

1. Appendix C: Cyber Systems Engineering

|  |  |  |
| --- | --- | --- |
| **CSYS Capabilities** | | |
| **Type** | **Area** | **Description** |
| System Settings | Computer System | * Retrieve windows operating system settings * Retrieve any client requested specific files |
| Reports | Client (workstation) Health | * Reporting of specified configuration settings related to the health of the client systems which could affect proper SCCM and HBSS functionality * Examples:   + Validation of local SMS Certificates   + Available Drive space   + Pending reboots   + Last System Restart date   + DNS client configuration   + SCCM Site Code   + Correct AD Site Name   + Windows Services Configuration   + Remote Registry Access   + SCCM Client Installation |
| Installed Application | * Report applications that appear to be non-standard installs on individual client Servers and Workstations * Examples:   + Unauthorized software installation enumeration   + Software versions   + Number of installations across client base   + Shareware/Freeware * Deliver monthly software installation reports for individual client workstations * Deliver lists of non-standard software to client for removal and resolution of possible issues on individual machines |
| Group Policy (GPO) | * Deliver reports of DISA STIG NON-IAVA, Air Force Guidance, and best practice findings contained within the Assessment Checklists that are actionable via a properly applied GPO * Check for correct settings of GPO * Check for compliance and best practice controls of GPO * Findings will indicate (where possible) what GPO (if any) are applied and whether or not their settings are correct |
| Account | * Reporting of all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to User and Local accounts * Reporting of dated Administrator accounts that need to be removed |
| Compliance and Health | Database | * Inspection of database compliance and health for all DISA NON-STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related database (SQL) systems * Examples:   + Validation that base is not using default or weak passwords for the SA Account   + Validations that Active Scripting Jobs and CmdExec jobs are restricted to SysAdmins   + Validation that SQL object permissions are not assigned to PUBLIC or GUEST * Provide optimization and stability * Scanning for any security issues * Provide individual checks on databases * Usage of Premier in-house built tools to perform compliance and health checks |
| DHCP | * Inspection of server compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to DHCP Server * Example:   + DHCP Lease Times   + Deactivated DHCP Scopes   + DHCP Server and Scope Option configurations   + DHCP Server side IP address conflict detection   + MAC Address mismatches between multiple DHCP Servers   + DHCP Scope Utilization   + Overall DHCP utilization   + “Rogue” DHCP Server identification   + DHCP Auditing   + DHCP redundancy   + Validation of DHCP reservations * Provide optimization and stability * Scanning for any security issues * Provide individual checks on servers * Usage of Premier in-house built tools to perform compliance and health checks |
| Active Directory | * Inspection of Active Directory Service compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to the Active Directory Service * Examples:   + Validation of domain functional level is compliant   + Validation of physical server configurations for Active Directory Servers   + Validation of AD sites and services configuration settings   + Validation of Active Directory logging   + Validation of correct FSMO role placement   + Validation that critical Windows Services are configured and running correctly   + Validation of AD Site Link Configurations   + Validation of AD Replication is configured and occurring   + Validation that workstations and servers are being assigned the correct AD Site Code   + Validation of LDAP configuration settings   + Validation of Machine account settings   + Validation of Windows Time Service configurations   + Validations that Stale Computer and user accounts are removed from Active Directory   + Validation of Active Directory Domain Trusts are configured correctly   + Validation of AD schema security settings   + Validation of PKI certification configurations   + Validation of DoD required password complexity implementation * Provide optimization and stability * Scanning for any security issues * Provide individual checks on Active Directory Service * Usage of Premier in-house built tools to perform compliance and health checks |
| DNS | * Inspection of DNS compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to DNS * Examples:   + Validation that DNS Services are only installed on authorized servers   + Validation that workstation and servers are correctly configured to use authorized DNS servers   + Validation that Dynamic updates are cryptographically authenticated   + Validation that Zone transfers are prohibited (or a VPN solution is implemented) that requires cryptographic authentication of communicating devices and is used exclusively by name servers authoritative for the zone   + Validation of Zone Security   + Validation that DNS listener interfaces are configured correctly   + Validation that DNS Solution satisfied the security requirements of the STIG   + Validation of Zone Transfer security settings   + Validation that Reverse lookup zones exist for the site IP space   + Validation that Root Hints are not used   + Validation of specific server settings for servers hosting DNS service   + Validation of DNS logging   + Validation that necessary records are registered in DNS   + Validation that aging and scavenging is properly configured * Provide optimization and stability * Scanning for any security issues * Provide individual checks on DNS * Usage of Premier in-house built tools to perform compliance and health checks |
| Messaging/Exchange | * Inspection of Messaging (Exchange) compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to Messaging (Exchange) * Provide optimization and stability * Scanning for any security issues * Provide individual checks on Messaging/Exchange * Usage of Premier in-house built tools to perform compliance and health checks |
| Operating System | * Inspection of workstations and servers compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to Workstations or Servers * Examples:   + Validation that Administrator automatic logons are disabled   + Validation that non-administrators are prevented from applying vendor-signed updates   + Validation that network shares that can be accessed anonymously do not exist   + Validation that the Windows Registration Wizard is turned off   + Validation that Windows Media Player is configured to prevent automatic checking for updates   + Validation that USB flash drives have not been connected to DoD systems   + Validation that event log sizes meet minimum requirements   + Validation that Remote Desktop Services will delete temporary folders when a session is terminated   + Validation that systems have the DNS Client service started   + Validation that Windows systems are prevented from using Windows Update to search for drivers * Provide optimization and stability * Scanning for any security issues * Provide individual checks on workstations and servers * Usage of Premier in-house built tools to perform compliance and health checks |
| SCCM Server | * Inspection of servers compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to SMS/SCCM * Examples:   + Validation that SCCM clients are pointing to the correct server/site   + Validation of proper AD configuration   + Validation of SCCM identifiers   + Validation of Package Configurations * Provide optimization and stability * Scanning for any security issues * Provide individual checks on servers * Usage of Premier in-house built tools to perform compliance and health checks |
| WebServer | * Inspection of servers compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to Web Servers (IIS) * Examples:   + Validation of Web Server permissions   + Validation that all installed utilities and programs are necessary for operations   + Validation that Directory Browsing is disabled   + Validation of service account password compliance   + Validation for the presence of DoD PKI Server certificate   + Validation that number of simultaneous requests are configured correctly   + Validation of backup interactive scripts are prohibited   + Validation that only necessary services are installed and running   + Validation that logging is correctly configured   + Validation that shares are correctly configured   + Validation that the II 6.0 metabase is being backed up   + Validation that FTP Server is properly configured for security   + Validation that anonymous access accounts are restricted * Provide optimization and stability * Scanning for any security issues * Provide individual checks on servers * Usage of Premier in-house built tools to perform compliance and health checks |
| WINS | * Inspection of WINS compliance and health for all DISA STIG NON-IAVA, AF Guidance, and best practice findings contained in the Assessment Checklists related to WINS * Examples:   + Validation that correct ration of WINS Servers vs clients is correct   + Validation of WINS replication partners   + Validation of default WINS configuration   + Validation of WINS database backups and scavenging   + Validation that a hub and spoke design model are being used   + Validation that workstations are configured to use authorized WINS servers   + Validation that logging is configured correctly   + Validation that WINS service is installed only on authorized WINS servers   + Validation that replication partners are configured to be Push/Pull   + Validation that Database Consistency Checking is enabled and configured correctly * Provide optimization and stability * Scanning for any security issues * Provide individual checks on WINS * Usage of Premier in-house built tools to perform compliance and health checks |

1. Appendix D: Cyber Network Engineering

|  |  |  |
| --- | --- | --- |
| **CNET Capabilities** | | |
| **Type** | **Area** | **Description** |
| Battle-space Reconnaissance | Infrastructure Router/Switches | * Ping sweeps * Targeting Port sweeps * Testing SNMP * Developing target lists * Fingerprinting Operating Systems * Validating Active Devices * Discovering Networks * Validating expected configurations * Discovering CDP/LLDP networks * Validating credentials * Validating access * Confirming target lists * Versioning Operating Systems |
| Virtualized Server Infrastructure (VMWare/HyperV) | * Developing target lists * Fingerprinting Operating Systems * Validating Active Devices * Discovering Networks * Validating expected configurations * Validating credentials * Validating access * Confirming target lists * Versioning Operating Systems |
| Network Management Servers | * Targeting Port sweeps * Testing SNMP * Developing target lists * Fingerprinting Operating Systems * Validating Active Devices * Validating expected configurations * Validating credentials * Validating access * Confirming target lists * Versioning Operating Systems |
| Authentication, Authorization, & Accounting Services | * Targeting Port sweeps * Developing target lists * Fingerprinting Operating Systems * Validating Active Devices * Validating expected configurations * Validating credentials * Validating access * Confirming target lists * Versioning Operating Systems |
| Target Data Acquisition | Infrastructure Router/Switches | * Gathering Bulk data * Gathering performance statistics via pre-built tools * Analyzing data set for additional likely targets not previously detected * Logging file sources |
| Virtualized Server Infrastructure (VMWare/HyperV) | * Gathering Bulk data * Gathering performance statistics via pre-built tools * Triaging tools to evaluate gathered data for common import failures * Gathering metadata source * Gathering baseline compliance source |
| Network Management Servers | * Analyzing data set for additional likely targets not previously detected * Logging file sources * Gathering metadata source * Gathering baseline compliance source |
| Authentication, Authorization, & Accounting Services | * Gathering Bulk data * Triaging tools to evaluate gathered data for common import failures * Analyzing data set for additional likely targets not previously detected * Logging file sources * Gathering metadata source |
| Target Data Pre-Processing | Infrastructure Router/Switches | * Parses bulk data files and loads into a consolidated database * Parses bulk data files and loads into a standalone database |
| Virtualized Server Infrastructure (VMWare/HyperV) | * Parses bulk data files and loads into a consolidated database * Parses bulk data files and loads into a standalone database |
| Authentication, Authorization, & Accounting Services | * Parses bulk data files and loads into a consolidated database * Parses bulk data files and loads into a standalone database |
| Battle-space Profiling and Analysis | Infrastructure Router/Switches | * Aggregating bulk data * Correlating target data across multiple data elements to assemble metadata * Analyzing key cross-vendor target parameters in near real-time * Real-time multi-vendor analysis of network traffic, bandwidth utilization, and data flow |
| Virtualized Server Infrastructure (VMWare/HyperV) | * Aggregating bulk data * Correlating target data across multiple data elements to assemble metadata * Analyzing key vendor-specific target parameters |
| Network Management Servers | * Aggregating metadata * Correlating target metadata across multiple management tools * Analyzing key target parameters * Providing near real-time vendor-specific and vendor-neutral analysis logic and situational awareness * Providing real-time vendor-specific and vendor-neutral analysis of network traffic, bandwidth utilization, and data flow |
| Authentication, Authorization, & Accounting Services | * Aggregating bulk data * Correlating target data across multiple data elements to assemble metadata |
| Battle-space Reporting | Infrastructure Router/Switches | * Providing primary findings in parsed, deliverable format, presorted and enumerated for actionable tasks to technical staff * Providing interim reports on selected items for immediate tasks * Producing basic and complex network mapping tools that export target data to Visio diagrams * Providing graphs and supporting data on key elements of interest * Producing custom reports from vendor-specific tools * Developing compliance reports |
| Virtualized Server Infrastructure (VMWare/HyperV) | * Providing primary findings in parsed, deliverable format, presorted and enumerated for actionable tasks to technical staff * Providing interim reports on selected items for immediate tasks * Reporting with vendor specific tools * Developing compliance reports |
| Network Management Servers | * Providing primary findings in parsed, deliverable format, presorted and enumerated for actionable tasks to technical staff * Providing interim reports on selected items for immediate tasks * Reporting with vendor specific tools * Tracking user and device location and status with vendor-specific and vendor-neutral tools * Developing compliance reports |
| Authentication, Authorization, & Accounting Services | * Providing primary findings in parsed, deliverable format, presorted and enumerated for actionable tasks to technical staff * Providing interim reports on selected items for immediate tasks * Auditing and accounting of commands and activities * Reporting with vendor specific tools * Tracking with user and device tools * Developing compliance reports |
| Battle-space Active Response | Infrastructure Router/Switches | * Deploying commands across multiple vendor platforms with custom remediation scripts developed on-site by analyst teams * Assisting sites with deploying individual or network-wide changes to systems based on deltas from authoritative baseline standards |
| Virtualized Server Infrastructure (VMWare/HyperV) | * Assisting sites with deploying individual or network-wide changes to systems based on deltas from authoritative baseline standards |
| Network Management Servers | * Assisting sites with development of centralized policy management systems to automatically validate network compliance with authoritative baseline standards * Assisting sites with implementing centralized management tools to deploy automated changes to systems based on deltas from authoritative baseline standards baseline standards |
| Authentication, Authorization, & Accounting Services | * Assisting sites with development of centralized policy management systems to automatically enforce authoritative access policies |