CASSIE The Consortium for the Analysis of Student Success through International Education

Data Privacy and Security Practices

Alfred Barker

Assistant Vice Chancellor, Chief Information Security Officer

Contributors,
Dr. Gregory Shutz – Assistant Vice Chancellor for Strategic Business Intelligence
Greg Turmel – Director Data Warehouse

USG Cybersecurity

PROTECTION IS IDEAL BUT DETECTION IS A MUST!

EXECUTIVE SUMMARY

CASSIE is led by the University System of Georgia (USG) in coordination with the Institute of International Education and funded by the U.S. Department of Education's International and Foreign Language Education Office. It is a research project to study the impact of international education experiences (e.g. study abroad, taking a foreign language, Title VI program participation) on a variety of student success outcomes.

The research project will create a database in the USG data warehouse (USGDW) of de-identified student-level data from both USG and non-USG colleges and universities that includes information on student demographics, academic characteristics, international experiences, and educational outcomes.

The USG data warehouse currently securely stores student data for the 26 institutions of the USG and grants access to designated role-based users. Data are not stored on local devices or within computer tools/applications.

Data security is foundational to CASSIE and will be assured through the following operational processes and technical, physical, and administrative cybersecurity safeguards:

- USG data warehouse personnel will utilize current warehouse loading, storage, and access procedures and technologies to provide services for the CASSIE project.
- Data are stored in an Oracle 12.1.02 database managed and monitored with Oracle Enterprise Manager 13C.
- The database is protected by a next-generation Palo Alto firewall that allows connections only to defined and authorized IP address ranges.
- Individuals (no shared accounts) access the warehouse with Active Directory accounts associated with designated role-based security. All accounts are re-certified on an annual basis.
- Oracle Transparent Database Encryption (TDE) is used to encrypt all sensitive data at the database table level.
- Oracle SQLNET Encrypted connections are used and required to encrypt all data during transport across the network.
- The USG environment is actively being monitored by the enterprise security operations center.
- The data warehouse is protected through enterprise backup and recovery operations.
- The data are physically protected in a secure data center using biometric controls to restrict access to only authorized personnel.
- Protection of sensitive data is fostered through administrative controls in the form of comprehensive actions, policies, and procedures.

Transmission of datasets from participating institutions will be carried out by the USG's secure file transfer utility system, MoveIT. Secure access to the CASSIE databank is in place through Toad database administration software. Statistical analyses will be carried out via STATA and SPSS software.

The purpose of this assessment is to describe the operations and safeguards in place to protect the project's de-identified student data once stored and secured with access only granted to designated CASSIE researchers. Also reviewed is the security of both the computing tools (computer and any digital storage device) and the physical space (e.g. data on servers in locked area, building is accessible only to people with USG ID, etc.) that will be involved in the data storage.

INTRODUCTION

The Consortium for Analysis of Student Success through International Education (CASSIE) project is led by the University System of Georgia (USG) Research and Policy Analysis division (RPA). It is being carried out in coordination with the Institute of International Education and is funded by the U.S. Department of Education's International and Foreign Language Education Office. It is a research project to study the impact of international education experiences (e.g. study abroad, taking a foreign language, Title VI program participation) on a variety of student success outcomes.

The research project will create a database in the USG data warehouse (USGDW) of de-identified student-level data from both USG and non-USG colleges and universities that includes information on student demographics, academic characteristics, international experiences, and educational outcomes.

The USG data warehouse currently securely stores student data for the 26 institutions of the USG and grants access to designated role-based users. Data are not stored on local devices or within computer tools/applications. Data security is assured through operational processes and cybersecurity safeguard that will be detailed in this document.

Transmission of datasets from participating institutions will be carried out by the USG's secure file transfer utility, MoveIT. Secure access to the CASSIE databank is in place through Toad database administration software. Statistical analyses will be carried out via STATA and SPSS software.

I. OPERATIONS

USG data warehouse personnel will utilize current warehouse loading, storage, and access procedures and technologies to provide services for the CASSIE project.

USGDWH ADDENDUM PROCESS FOR CASSIE SCHEMA

1.0.1 Diagram 'USG Warehouse 12c Schema Layout' under Data Layer

- Modify artifact to include CASSIE Schema

1.0.2 Diagram 'USG Warehouse 12c Schema Layout' under Source Systems

- Modify artifact to include MoveIT for CASSIE files

1.0.3 Diagram 'USG Users and Groups' under Users and Groups

- Assumption: Adopt existing USG Users and Groups Security Architecture, Lighweight Directory Access Protocol (LDAP) roles, and Enterprise User Security Roles core designs
- Under LDAP roles: Modify user and groups to isolate the selected researchers
- Modify LDAP roles to isolate the CASSIE reviewers
- Under Enterprise Users Security Roles: Modify Oracle Unified Directory/Oracle Internet Directory (OUD/OID) user security roles to isolate CASSIE reviewers

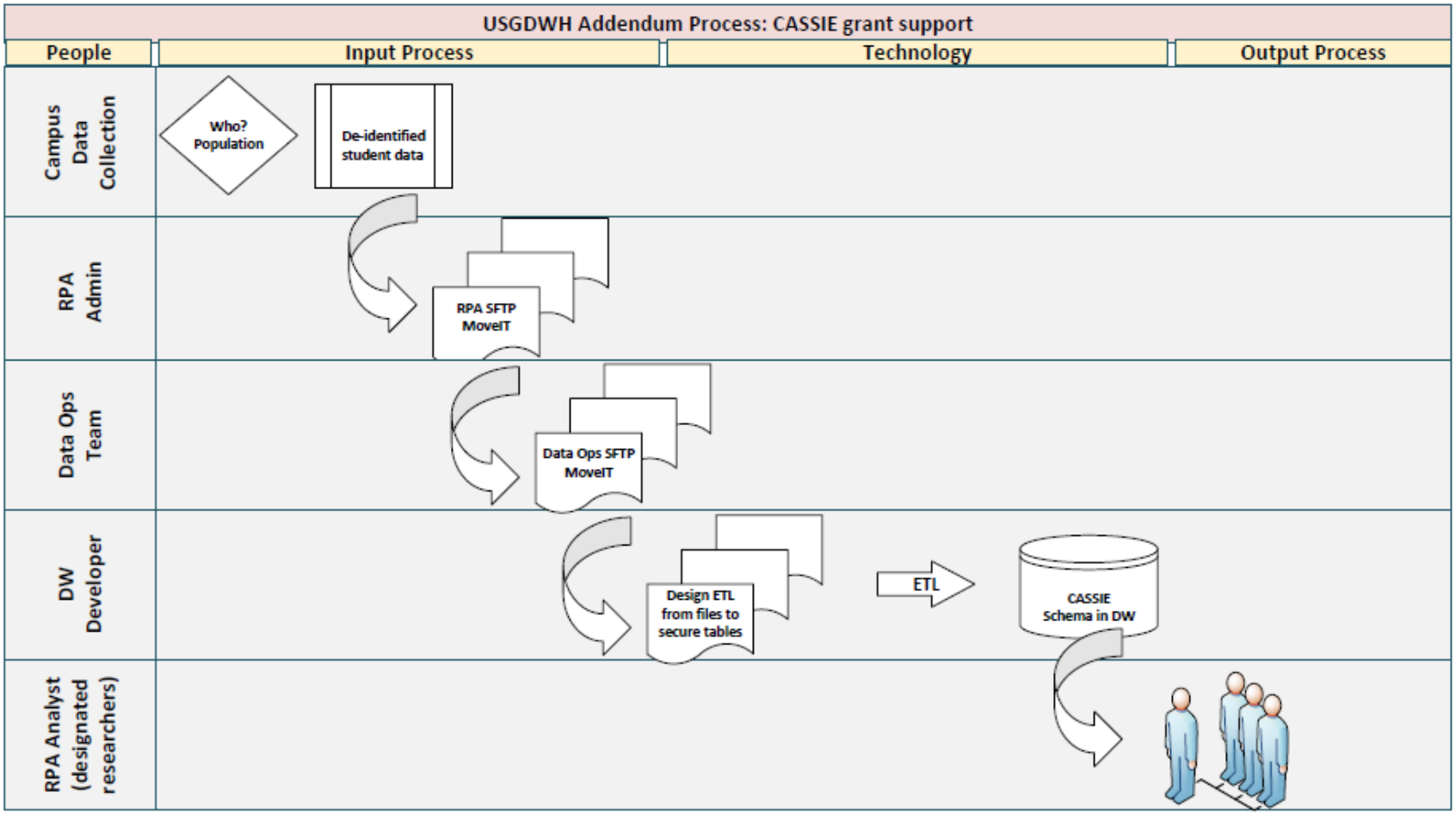
1.0.4 Diagram 'USG Data Warehouse Security Architecture Virtual Data Protection (VDP) Security'

- Assumption: Adopt existing USG VDP Security profile
- Modify VDP to isolate CASSIE reviewers

1.0.5 List: 'USG Date Warehouse Inventory'

- Assumption: No additional hardware inventory changes are required to support the collection

Figure 1: USGDW Addendum Process for CASSIE Project



Assumptions:

1. Data Stored in and Oracle 12c database managed and monitored with Oracle Enterprise Manager 13c.
2. The database is protected by a next generation Palo Alto firewall that allows connections only to defined and authorized IP address ranges.
3. Individuals (no shared accounts) will access the warehouse with Active Directory accounts associated with designated role-based security.
4. All accounts are re-certified on an annual basis.
5. Oracle Transparent Database Encryption (TDE) is used to encrypt all sensitive data at the database table level.
6. Oracle SQLNET encrypted connections are used and required to encrypt all data during transport across the network.
7. The data are physically protected in a secure data center using biometric controls to restrict access to authorized personnel only.
8. Data element definitions are pre-determined by tables selected for collection and then replicated in warehouse (does not require designing/developing tables or DED).
9. Data selection criteria pre-determined by specifications used by researchers.
10. Data de-identified prior to leaving source location and securely sent to RPA using RPA MoveIT folders for campus.
11. RPA MoveIT secure file transfer protocol can securely move the submissions to the DW Data Ops MoveIT folder for processing.
12. Database administrators, Data Ops, and USGDW developer teams (due to positions) will be in the 'authorized' team assisting RPA Analysts securing project.

People	Process	Technology	Input / Output
Campus	Selecting population	SFTP via MoveIT	in
RPA	Rec'd submission / send to DW team	SFTP via MoveIT	In / out
USG Data Ops	Rec'd submission / work with DBA's	SFTP via MoveIT	In / out
USG DBAs	Stage files on DB server	TBD	In
USG Developers	ETL from files to tables	ODI from dat files	In / out to tables
Selected Analysts	Query access	TOAD	Out to analytics reports

Table 1. Process Structures

The USG data warehouse securely stores sensitive data and grants access to designated role-based users. Data are not stored on local devices or within computer tools/applications. Data security is assured through the following provisions:

- Data are stored in an Oracle 12.1.02 database managed and monitored with Oracle Enterprise Manager 13C.
- The database is protected by a next-generation Palo Alto firewall that allows connections only to defined and authorized IP address ranges.
- Individuals (no shared accounts) access the warehouse with Active Directory accounts associated with designated role-based security. All accounts are re-certified on an annual basis.
- Oracle Transparent Database Encryption (TDE) is used to encrypt all sensitive data at the database table level.
- Oracle SQLNET Encrypted connections are used and required to encrypt all data during transport across the network.
- The USG environment is actively being monitored by the enterprise security operations center.
- The data warehouse is protected through enterprise backup and recovery operations.
- The data are physically protected in a secure data center using biometric controls to restrict access to only authorized personnel.

TREND ANALYSIS

ITS Technical Operations employs a sophisticated trend analysis service[1] that continuously collects hundreds of data points about ITS managed servers. In addition to its use in active trouble-shooting, the tool is used to analyze historical trends, to predict and avoid problems, and to inform future purchases.

SUPPORT

ITS Technical Operations maintains active support and maintenance contacts with our operating system and hardware vendors. In addition to providing for timely on-site support for hardware troubleshooting and replacement, these contracts ensure access to the latest version of software and operating system updates including vendor security patches and updates.

[1] Yakety Stats – proprietary build solution

II. CYBERSECURITY SAFEGUARDS

Cybersecurity at USG is considered to be the policies, guidelines, best practices, security concepts, security safeguards, risk management approaches, actions, training, tools, and technologies that are used to protect the cyber environment and and the organization's and user's assets.

A. TECHNICAL CONTROLS

USG employs technical security controls that the computer system executes. These controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

SECURITY OPERATIONS CENTER

The USG Cybersecurity Enterprise Security Operations Center (SOC) utilizes Dell SecureWorks' Managed Security Services primarily out of their Atlanta SOC. SecureWorks four SOCs – Atlanta, Chicago, Myrtle Beach and Providence – are completely synchronous; all critical information systems are mirrored at each location and critical cybersecurity data are replicated between these SOCs in real time, creating an environment that ensures uninterrupted 24x7x365 service delivery uptime under all circumstances. SecureWorks SOCs are completely self-sufficient and operate from carrier-grade facilities that have redundant ISP connections, backup power generators and redundant systems to maintain service delivery for all Clients without additional support.

Physical security measures deployed at our SOCs include:

- Multi-factor authentication (keycard and passcode, keycard and biometric) at entrance doors and critical areas, such as the SOC and data center; keycard access required for all other areas
- Video surveillance
- 24x7x365 monitoring of all physical security mechanisms
- High-availability telecommunications
- Multiple power grids with failover capabilities
- Facilities with generator systems configured to provide power to the SOCs in the event of a total power outage.
    - Self-test is performed on a weekly basis
- Redundant environmental control systems
- Fire detection and Halon-based suppression systems

Event Handling Process

SecureWorks' Event Handling Process is a clearly defined method for incident identification and response that complements USG efforts. USG Cybersecurity uses the SecureWorks Client Portal to contribute feedback, which is then incorporated into future revisions of the Event Handling Process, which includes:

- Correlation of security events
- Validation of security events
- Trend analysis of security events

- Escalation of security incidents
- Retention of security events

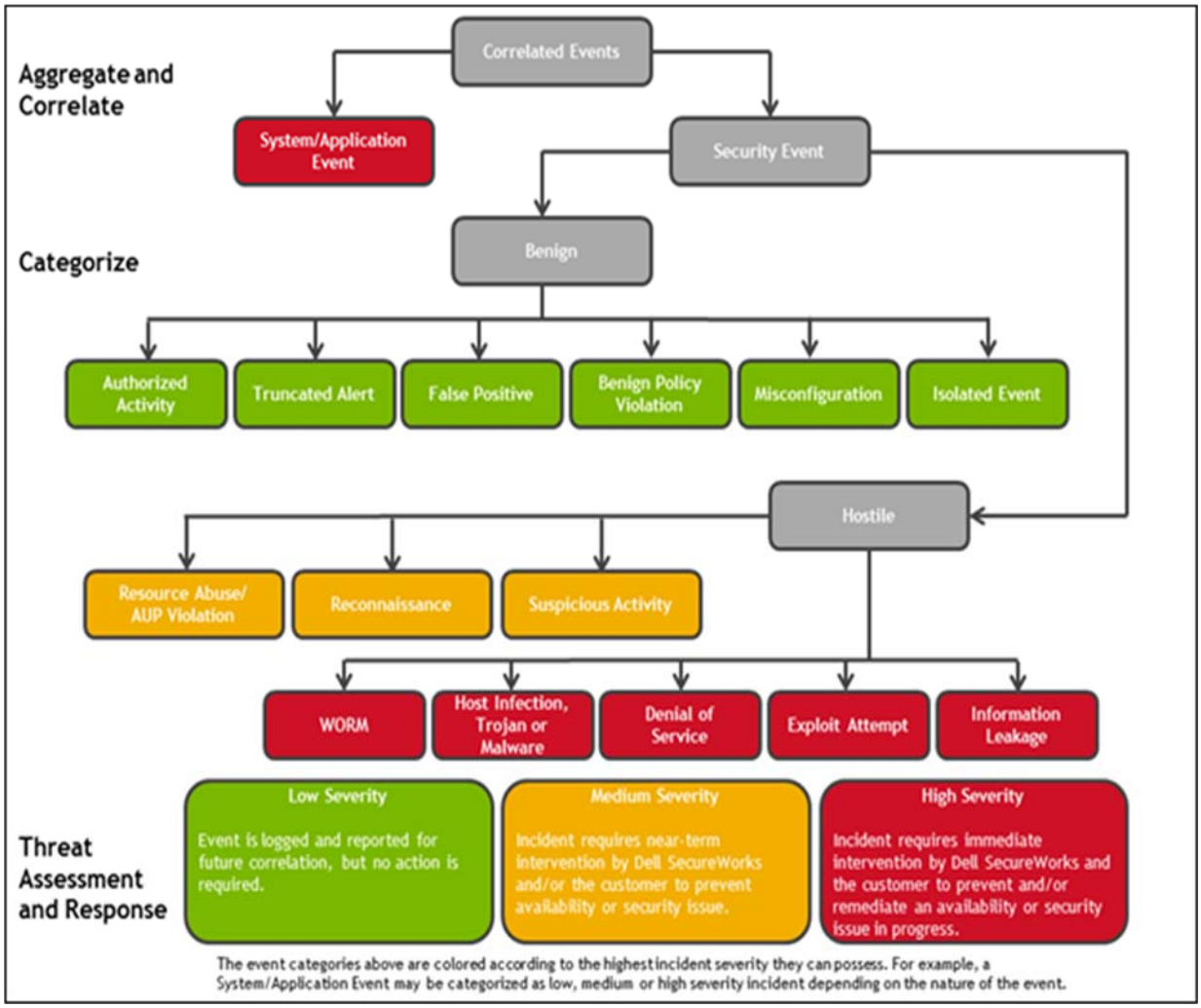


Figure 2: Event Handling Process

Security Intelligence and Perspectives

Secure Works' Theat and Vulnerability Management Dashboard displays customizable information specific to USG Cybersecurity personnel job responsibilities in addition to a variety of predefined charts, maps, and data grids.

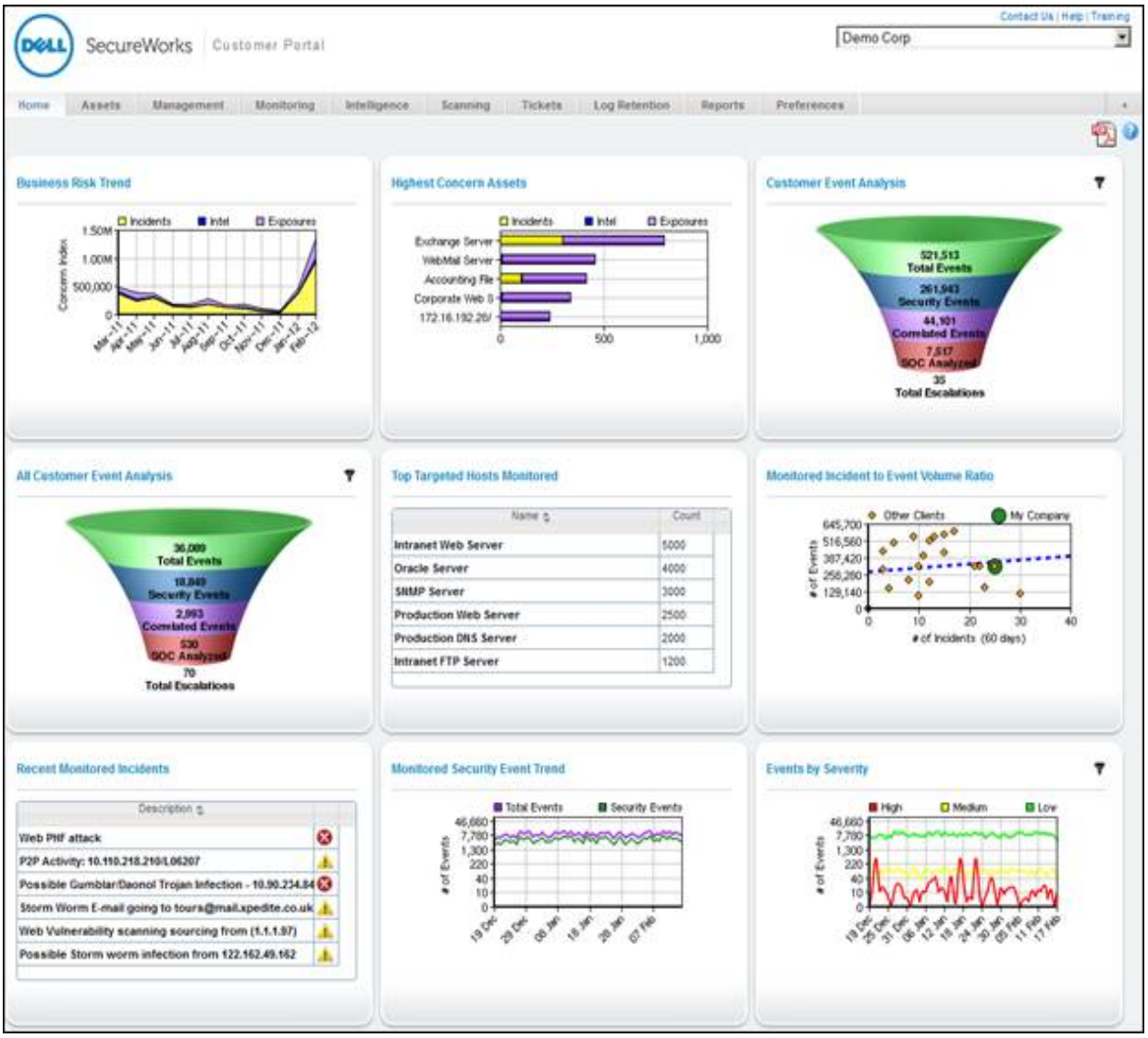


Figure 3: Threat and Vulnerability Management Dashboard

Detailed Analytical Tools

USG's portal data analysis tools provide advanced drill-down capabilities, allowing USG Cybersecurity to develop deep analysis of the USG's protected data. The Real-Time Event Monitoring Portal screenshot above allows USG Cybersecurity to view security events in real time.

Managed iSensor Intrusion Prevention System (IPS)

USG utilizes SecureWorks' managed iSensor IPS service, available as a fully managed intrusion prevention service and as an enterprise-level bundle. It helps eliminate malicious inbound and outbound traffic around the clock, without the burden of device or signature management, and without increasing in-house headcount. The iSensor utilizes thousands of unique countermeasures developed by SecureWorks Counter Threat Unit research team. Service features include:

- Configuration and implementation
- Administration and tuning

- 24x7x365 real-time security event and device health monitoring
- Upgrade, change and patch management
- Thousands of unique iSensor countermeasures
- Daily audits of existing iSensor rules
- Advanced analysis and blocking techniques
- Advanced statistical analysis
- Suspicious activity correlation and expert security analysis of patterns
- Twice weekly countermeasure updates
- Intelligence-enhanced threat protection
- On-demand security and compliance reporting

The Counter Threat Appliance

The USG also has implemented Counter Threat Appliance (CTA), which resides on USG's PeachNet network and is responsible for maintaining connections to all sources USG needs monitored and managed. USG's PeachNet is the network over which all USG traffic moves.

Log Monitoring

SecureWorks' Log Monitoring service provides 24x7x365 vigilance over security devices and critical information assets. The service monitors, analyzes, and responds to security events from the USG environment in real time.

Service features include:

- Expert log and event analysis by Security Analysts
- Vendor-neutral, infrastructure-wide coverage
- Real-time, 24x7x365 monitoring, correlation and incident response
- Risk discovery with remediation details and workflow with ticketing
- On-demand security and compliance reports through real-time Client Portal

DATA CENTER

USG's Data Centers are managed by the University System Office's Information Technology Services (ITS). The two data centers are represented by roles, primary and failover. The ITS' primary Data Center in Athens, Georgia houses the server and networking components required to provide our services. A second facility, located at the University of Georgia, provides a failover location for the primary data center with redundant services utilizing active-active and active-standby models.

Backup and Recovery Service

ITS Technical Operations manages an enterprise backup and recovery service currently based on Dell EMC Avamar and Data Domain enterprise storage technologies. Backups run on every system at least once per 24 hours. All production backups stream automatically to an *off-site* data center. Standard backup retention is seven days for production servers and three days for non-production (development, test, etc.) servers.

Central Logging

In addition to local logs, all UNIX and Linux servers are configured to stream system log data to a central log management server. Log scanning software continuously runs on the central server to detect and alert about possible system problems.

Monitoring

ITS Technical Operations employs an enterprise monitoring system to actively monitor the state of all ITS managed servers and services. In addition to monitoring for possible problems related to service availability, memory utilization, CPU utilization, storage consumption, etc., the system also monitors to ensure that unsecure protocols such as TELNET, FTP, and HTTP are *not* running on any servers other than those on which they are expected. Critical alerts are sent to mobile devices carried by on-call staff who are available 24/7/365.

Central Configuration and System Management

ITS Technical Operations uses central configuration and system management tools (Puppet, Active Directory, Group Policies, and Red Hat Satellite Server) to ensure that all systems are updated routinely and consistently. Puppet in particular can reset certain accidental or malicious changes back to the correct system state.

Access Control

ITS Technical Operations uses a central directory infrastructure (LDAP and Active Directory) for account management, authentication, and authorization. This ensures consistent account authorization across systems. Conversely, it allows for quick and consistent user *termination* across all systems.

B. PHYSICAL CONTROLS

The protection of physical items, objects, or areas from unauthorized access or misuse.

ATHENS OFFICE

Physical access is restricted and controlled by a computerized access control system (Lenel). Access requires both a physical badge and successful biometric fingerprint.

The ambient environment for the Data Center is maintained by four Computer Room Air Conditioning units (CRACs), which provide for cooling, heating, humidification and dehumidification and maintain constant temperature and humidity to the equipment. The design is such that a planned or unplanned outage of one of the CRACs will not impact the ability to maintain the environment.

Fire protection is provided by smoke and heat sensors that will trigger a FM-200[2] fire-suppression in case of fire detection. A liquid detection system is used to detect water leakage into the Data Center.

Vigilant Camera systems are deployed with a DVR. Considered a compensating control, the camera system is used to ID intruders that by-pass standard entry protocol, trigger motion detection and is used to support investigations. The system is reviewed twice annually.

In addition, a compensating control, a burglar alarm system has been added independent of the Lenel entry system and is monitored by the EIS team.

[2] FM-200™ waterless extinguishes fires through a combination of chemical and physical mechanisms, an environmentally sound replacement for ozone damaging Halon.

UGA Facility

Access control is provided via UGA managed card/badge access and again a keycard to unlock the ITS equipment cage. The facility utilizes zones-of-trust model separating each user and the equipment away from other users. 24/7 managed facility.

Supplemental/Redundant Power

Power to all USG managed and leased Data Center services (servers and their support infrastructure) is protected by an Uninterruptable Power Supply (UPS), which conditions the power and provides for battery backup in case of input power failure.

Power to the building housing the DB300 Data Center is fed from two diverse paths into the campus, each of these paths being fed from diverse substations. Each of these two feeds are connected to an Automatic Transfer Switch (ATS), such that power to the building will automatically be reinstated from the alternate path within a few seconds of failure of the primary path. Additionally, if both of the normal paths fail, the utility provider can reconfigure each of these two paths to be fed from other substations. Within the DB300 building, the power feeding the Data Center's UPS, CRACs, fire protection systems, monitoring and other dependencies is further protected by a second ATS which, as a last line of defense, can auto-start and transfer the load to our Balor – Cummings Engine – natural gas generator.

Each of these Data Center-dependent systems is monitored by our Enterprise Infrastructure Team using an enterprise monitoring system[3] that provides historical data to our trend-analysis system[4].

C. ADMINISTRATIVE CONTROLS

Administrative controls are administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect regulated information.

Incident Management

Security incident management is handled through the USG Office of Information Security & ePrivacy. The incident response guidelines and reporting instructions are documented here:

- *http://www.usg.edu/infosec/incident_management* [1]

The Incident Management standard is located:

- *http://www.usg.edu/information_technology_handbook/section5/C2080* [2]

Password Policy

ITS Technical Operations follows the IT Handbook Section 5.12 Password Security Standard

- *http://www.usg.edu/information_technology_handbook/section5/C2267* [3]

In summary, passwords are never stored unencrypted. Enterprise Infrastructure Services enforce complex passwords that are at least 10 characters in length and that use at least three of the four character types of upper-case, lower-case, numbers, and special characters. Passwords must be changed at least every 180 days or are disabled.

---

[3] Nagios - https://www.nagios.com/

[4] Yakety Stats – proprietary build solution

POLICY COMPLIANCE AND MANAGEMENT

The USG Office of Information Security & ePrivacy has documented standards on IT Security here:

- *http://www.usg.edu/information_technology_handbook/* [4]

REFERENCES

[1] University System of Georgia, "IT Handbook Sec 5.3, Incident Management," 15 May 2017. [Online]. Available: http://www.usg.edu/information_technology_handbook/section5/C2080. [Accessed 14 December 2017].

[2] University System of Georgia, "Cyber Incident Management," USG Cybersecurity, 30 June 2017. [Online]. Available: http://www.usg.edu/infosec/incident_management. [Accessed 14 December 2017].

[3] University System of Georgia, "IT Handbook, Sec 5.12 Password Security," 17 May 2016. [Online]. Available: http://www.usg.edu/information_technology_handbook/section5/C2267. [Accessed 14 December 2017].

[4] University System of Georgia, "IT Handbook: Overview," 15 May 2017. [Online]. Available: http://www.usg.edu/information_technology_handbook/. [Accessed 14 December 2017].