ADMINISTRATIVE COUNCIL MINUTES

July 14, 2021

The Administrative Council met on Wednesday, July 14, 2021 at 9:00 a.m. in the Athens State Carter Gymnasium. Present were Ms. Pam Clark, Recorder; Dr. Joe Delap; Mr. Andrew Dollar; Dr. Keith Ferguson; Ms. Jackie Gooch; Mr. Jeffrey Guenther; Dr. Jim Kerner; Ms. Belinda Krigel; Dr. Kim LaFevor; Mr. Chris Latham, Ms. Sarah McAbee; Mr. Mike McCoy; Mr. Derrek Smith; Dr. Jackie Smith; Dr. Stephen Spencer; Dr. Lee Vartanian; Ms. Debra Vaughn; Dr. Philip Way; Dr. Catherine Wehlburg; and Dr. Lionel Wright. Dr. Rick Barth; Ms. Laken Cleveland, SGA President; Mr. Richard Collie; and Mr. Jonathan Craft were absent. Special guests were Mr. Bud Gifford, Mr. Damon Lares, and Mr. Gary McCullors.

Dr. Way convened the meeting at 9:00 a.m. and welcomed everyone. There were no corrections to the June minutes. Dr. Smith made a motion to approve the minutes and Dr. Kerner seconded the motion. The minutes were unanimously approved on a voice vote.

Dr. Way stated the focus of the meeting is Cybersecurity. Dr. Way turned the meeting over to Ms. Krigel, who presented a PowerPoint slideshow on the topic (Handout 1). She introduced the guests by stating their names, titles and job responsibilities. Members were divided into four groups for discussions on a scenario exercise (Handout 2).

A. Group 1 – Delap, Gifford, LaFevor, Lares and McCullors

- A gap analysis has already been done.
- A disaster response plan for cyber-attacks is part of a comprehensive business continuity management plan. Have we created scenarios to address a disaster response plan? Do we know what the plans are? Training and testing need to take place.
- We have a good, existing plan in place for IT in the case of an event that takes us offline. Could a comprehensive Business Continuity Management Plan (BCMP) be helpful?
    - Need continuous assessment of potential classes of threats, key stakeholders and point people, impact analysis.
    - Develop and short and long-term strategies.
    - Conduct impact analyses of each class of threat and mitigation plan.
    - Need broad communication to organizational members, and detailed communications with key stakeholders.
    - Need to continuously assess the plans in place and regularly test and audit for changes.

B. Group 2 – Gooch, Kerner, J. Smith, Spencer, Vaughn and Wright

- Discussed how the students would be affected. Students can get to their Bb containers, use the website and email. Can we continue to teach our courses?

- We need an incident response - a unified statement for students, the public, the Board. What is the faculty's role and what do they need to do? Need a consistent voice to let us know what we need to do going forward.

C. Group 3 – **Guenther, McCoy, D. Smith, Vartanian and Wehlburg**

- Does the campus have a viable continuity of operations plan or disaster plan? Yes, we believe so, but everyone is not sure what it looks like.

- Does the campus have a communication plan? Yes, an example was the 2011 tornadoes. We were able to communicate to students using social media platforms. The new EAB alert system (text messaging) might be an additional way to communicate with students in the event of a future emergency.

- Does each department have its own continuity of operations plan? No, not every department has a written plan. A template would greatly assist each department to write a continuity of operations plan.

- What steps are required if there is no viable data backup? Can we get "hotspots" out to students if they cannot access our network? Can we restore to a previous data point? How is data/information saved to off-campus locations?

- Can the campus operate without technology? No.

- Are the dependencies on the current technology infrastructure of the campus creating a blind trust of IT's ability to restore technology? In some cases, we moving to vendor-supported (SaaS) solutions, which allow for some responsibility to be shifted to other campus units or third-party, off-campus entities.

D. Group 4 – **Dollar, Ferguson, Latham, McAbee and Way**

- Unsure of the continuity of operations plan.
- Many systems used by offices are cloud-based and stored off-site.
- Managing communications – rely on cell phone trees to employees.

Ms. Krigel encouraged everyone to look at building a contingency plan for their departments. She thanked everyone for their feedback. The meeting adjourned at 10:33 a.m.

Respectfully submitted by: Pamela Clark

Handout 1: "Cybersecurity" PowerPoint Presentation
Handout 2: Scenario Discussion Exercise

CYBERSECURITY

Administrative Council
July 14, 2021
Belinda Krigel, Gary McCullors, Bud Gifford, Damon Lares

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

AGENDA

- Introductions
- What is Cybersecurity vs Information Security?
- Impact on Higher Education, what is the concern?
- “Who” does “What” in cybersecurity – NICE Framework
- State of Cybersecurity defenses at Athens State – technology, staff, and awareness
- Tabletop exercises - 15 minutes for completing the exercise, 10 minutes for each group to report (a standard report template will be provided).

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

CYBERSECURITY

Cybersecurity focuses on preventing and defending against attacks and unauthorized use of computer systems, including networks, programs and data.

INFORMATION SECURITY

Managing the requirements to ensure the confidentiality, integrity, and availability of data.

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

IMPACT ON HIGHER ED

- AT LEAST 26 RANSOMWARE ATTACKS INVOLVING 26 COLLEGES AND UNIVERSITIES AND 58 SCHOOL DISTRICTS IN 2020
- A RANSOMWARE EXPLOIT INVOLVES STEALING SENSITIVE INFORMATION AND BLOCKING ACCESS TO ESSENTIAL DATA AND SYSTEMS THROUGH ENCRYPTION

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

WHY WE SHOULD BE CONCERNED

- MALICIOUS SOFTWARE SUCH AS PYSA RANSOMWARE (PROTECT YOUR SYSTEM AMIGO)
- USES PHISHING EMAILS (OR BRUTE FORCE ATTACK/UNAUTHORIZED REMOTE DESKTOP PROTOCOL) TO STEAL CREDENTIALS TO ACCESS IT NETWORKS
- CRIMINALS CAN SPEND MONTHS UNDETECTED SNOOPING AROUND COMPROMISED NETWORKS TO DETERMINE VULNERABILITIES
- STEAL SENSITIVE INFORMATION AND BLOCK ACCESS TO ESSENTIAL DATA AND SYSTEMS THROUGH ENCRYPTION – HELD FOR RANSOM.
- NOT ONLY BLOCK ACCESS BUT ALSO THREATEN TO RELEASE SENSITIVE DATA TO DARK WEB/PUBLIC.

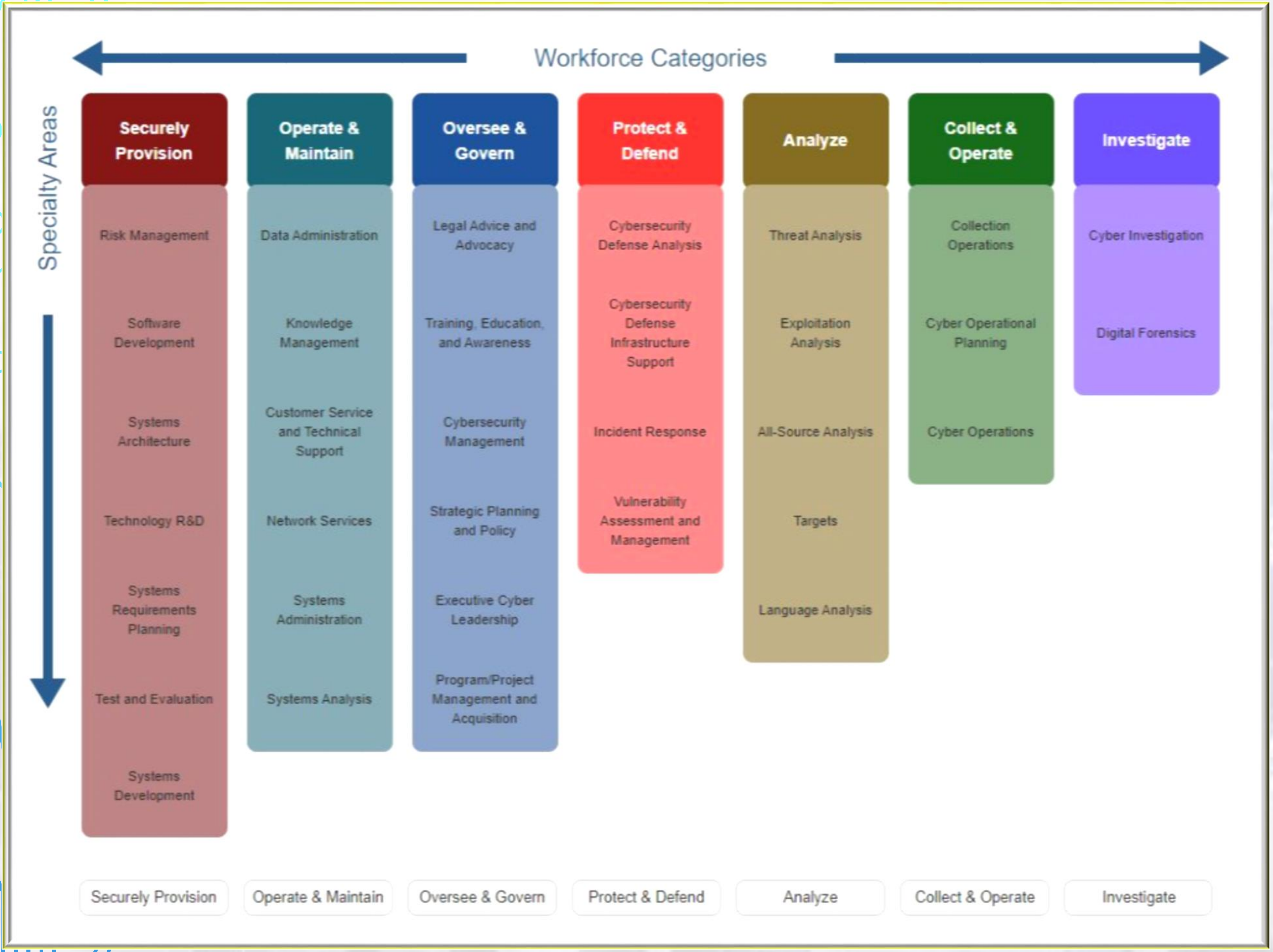
INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

- National Initiative for Cybersecurity Education (NICE) led by the National Institute of Standards and Technology (NIST).

- It is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.

INFORMATION
TECHNOLOGY
SERVICES
ATHENS STATE UNIVERSITY



Workforce Categories

Specialty Areas

Securely Provision	Operate & Maintain	Oversee & Govern	Protect & Defend	Analyze	Collect & Operate	Investigate
Risk Management	Data Administration	Legal Advice and Advocacy	Cybersecurity Defense Analysis	Threat Analysis	Collection Operations	Cyber Investigation
Software Development	Knowledge Management	Training, Education, and Awareness	Cybersecurity Defense Infrastructure Support	Exploitation Analysis	Cyber Operational Planning	Digital Forensics
Systems Architecture	Customer Service and Technical Support	Cybersecurity Management	Incident Response	All-Source Analysis	Cyber Operations	
Technology R&D	Network Services	Strategic Planning and Policy	Vulnerability Assessment and Management	Targets		
Systems Requirements Planning	Systems Administration	Executive Cyber Leadership		Language Analysis		
Test and Evaluation	Systems Analysis	Program/Project Management and Acquisition				
Systems Development						

Securely Provision | Operate & Maintain | Oversee & Govern | Protect & Defend | Analyze | Collect & Operate | Investigate

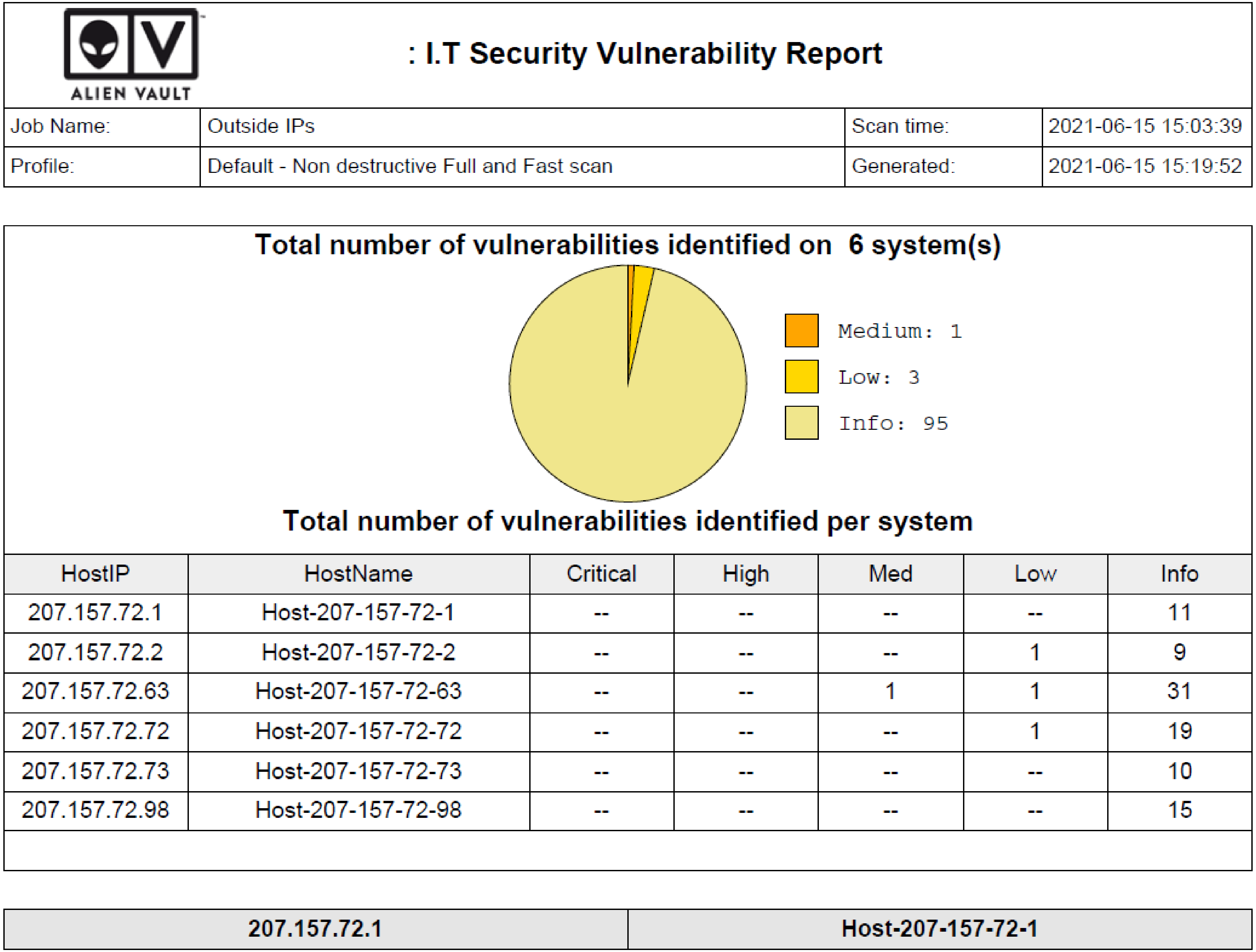
STATE OF CYBERSECURITY

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

STATE OF CYBERSECURITY

- Common Vulnerability and Exposure (CVE) scan
- Cyber Threat Assessment conducted by Fortinet

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY



ALIEN VAULT

: I.T Security Vulnerability Report

Job Name:	Outside IPs	Scan time:	2021-06-15 15:03:39
Profile:	Default - Non destructive Full and Fast scan	Generated:	2021-06-15 15:19:52

Total number of vulnerabilities identified on 6 system(s)

Total number of vulnerabilities identified per system

HostIP	HostName	Critical	High	Med	Low	Info
207.157.72.1	Host-207-157-72-1	--	--	--	--	11
207.157.72.2	Host-207-157-72-2	--	--	--	1	9
207.157.72.63	Host-207-157-72-63	--	--	1	1	31
207.157.72.72	Host-207-157-72-72	--	--	--	1	19
207.157.72.73	Host-207-157-72-73	--	--	--	--	10
207.157.72.98	Host-207-157-72-98	--	--	--	--	15

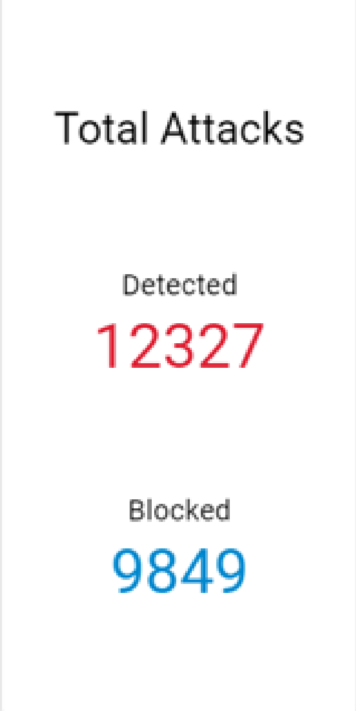
207.157.72.1	Host-207-157-72-1

CYBER THREAT ASSESSMENT

FROM 2021-06-21 THROUGH 2021-06-27

- IPS attacks detected: 62
- Malware/botnets detected: 1 (IoT Device)
- Websites visited: 41,236
- Malicious websites detected: 14
- Applications detected: 328
- High-risk applications used: 13
- Top website: usea1-012.sentinelone.net

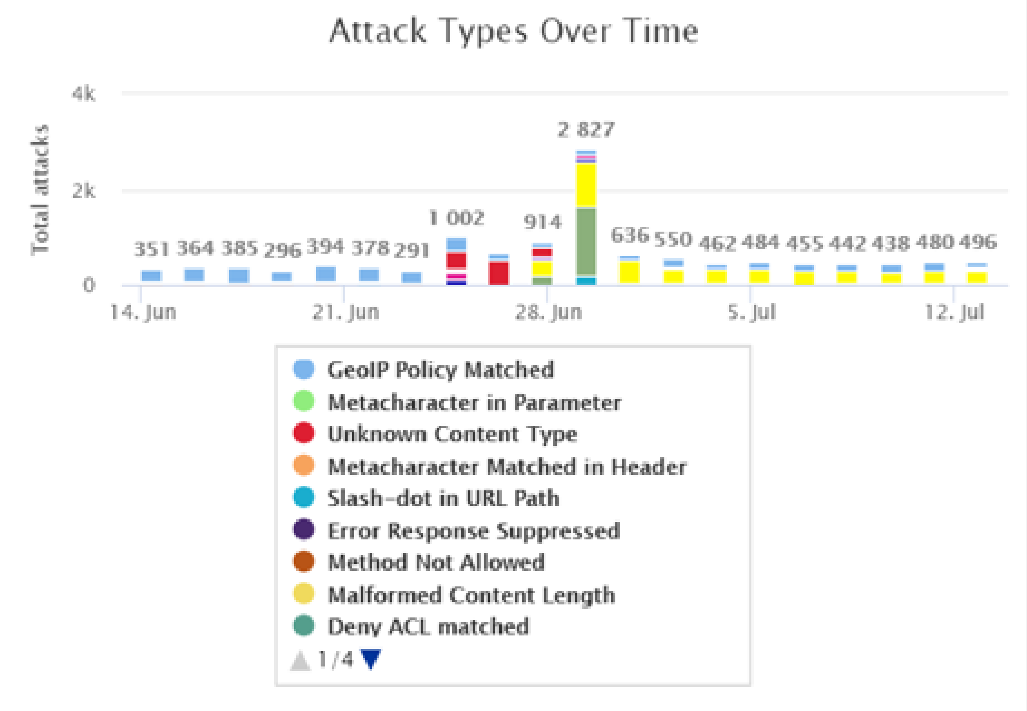
INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

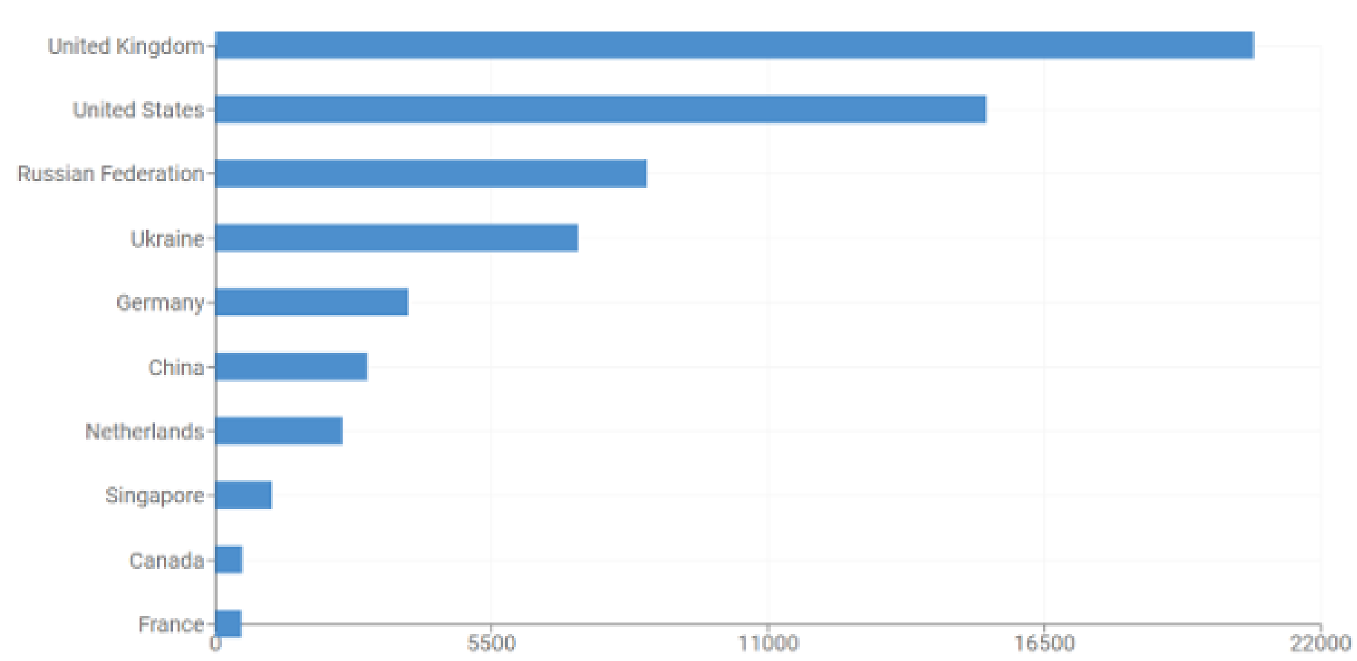


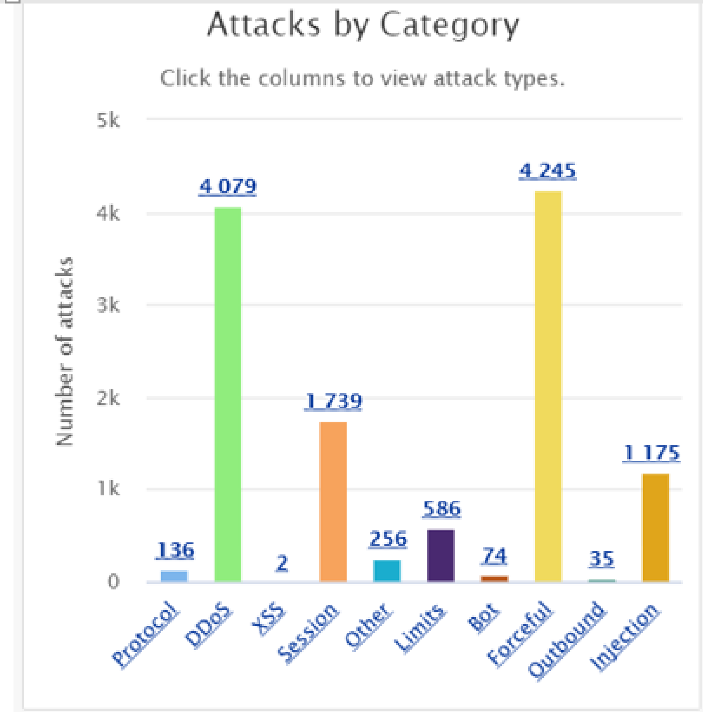
Total Attacks

Detected
12327

Blocked
9849

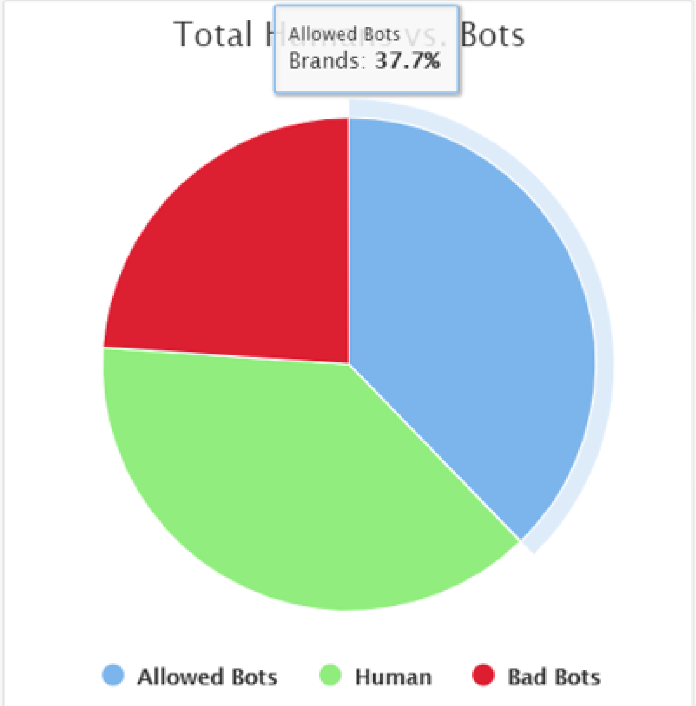






Attacks by Category

Click the columns to view attack types.



Total Human vs. Bots

CYBER THREAT ASSESSMENT

FROM 2021-06-21 THROUGH 2021-06-27

Overall assessment

(shoulder shrug)

…eh, we're ok…

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

SOME OF OUR CYBERSECURITY VULNERABILITIES

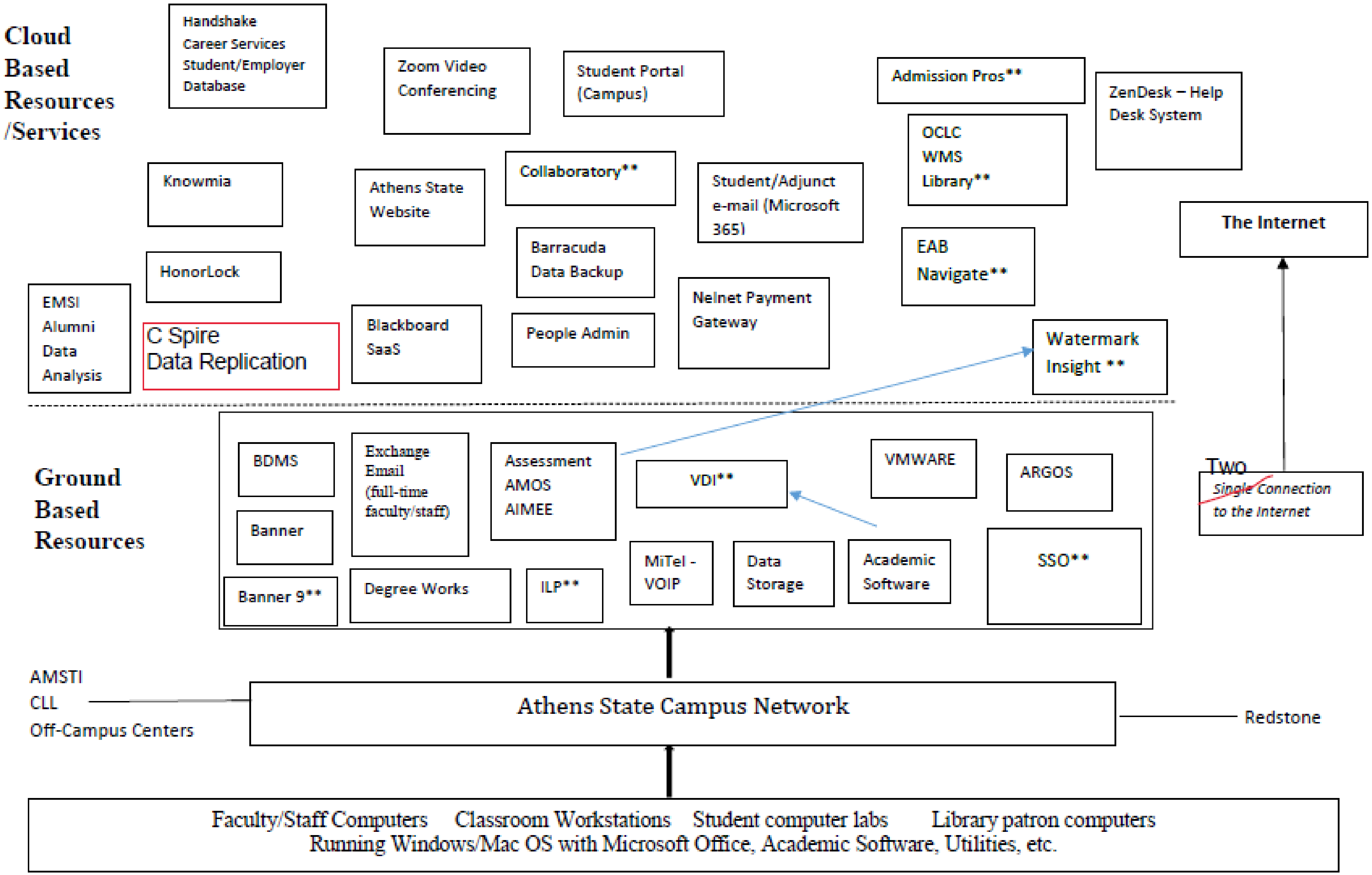
- Open campus and network environment
- Vendors and 3rd party associates
- Technology sprawl
- Network and data access control
- Passwords
- Awareness

Note – this list is not inclusive

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

Athens State University Information, Communication, and Instructional Technologies - 2021

**Implemented since 1/1/2020.



Cloud Based Resources /Services

Handshake Career Services Student/Employer Database

Zoom Video Conferencing

Student Portal (Campus)

Admission Pros**

ZenDesk – Help Desk System

OCLC WMS Library**

Knowmia

Athens State Website

Collaboratory**

Student/Adjunct e-mail (Microsoft 365)

The Internet

Barracuda Data Backup

EAB Navigate**

HonorLock

EMSI Alumni Data Analysis

C Spire Data Replication

Blackboard SaaS

People Admin

Nelnet Payment Gateway

Watermark Insight **

Ground Based Resources

BDMS

Exchange Email (full-time faculty/staff)

Assessment AMOS AIMEE

VDI**

VMWARE

ARGOS

Two ~~Single~~ Connection to the Internet

Banner

Banner 9**

Degree Works

ILP**

MiTel - VOIP

Data Storage

Academic Software

SSO**

AMSTI
CLL
Off-Campus Centers

Athens State Campus Network

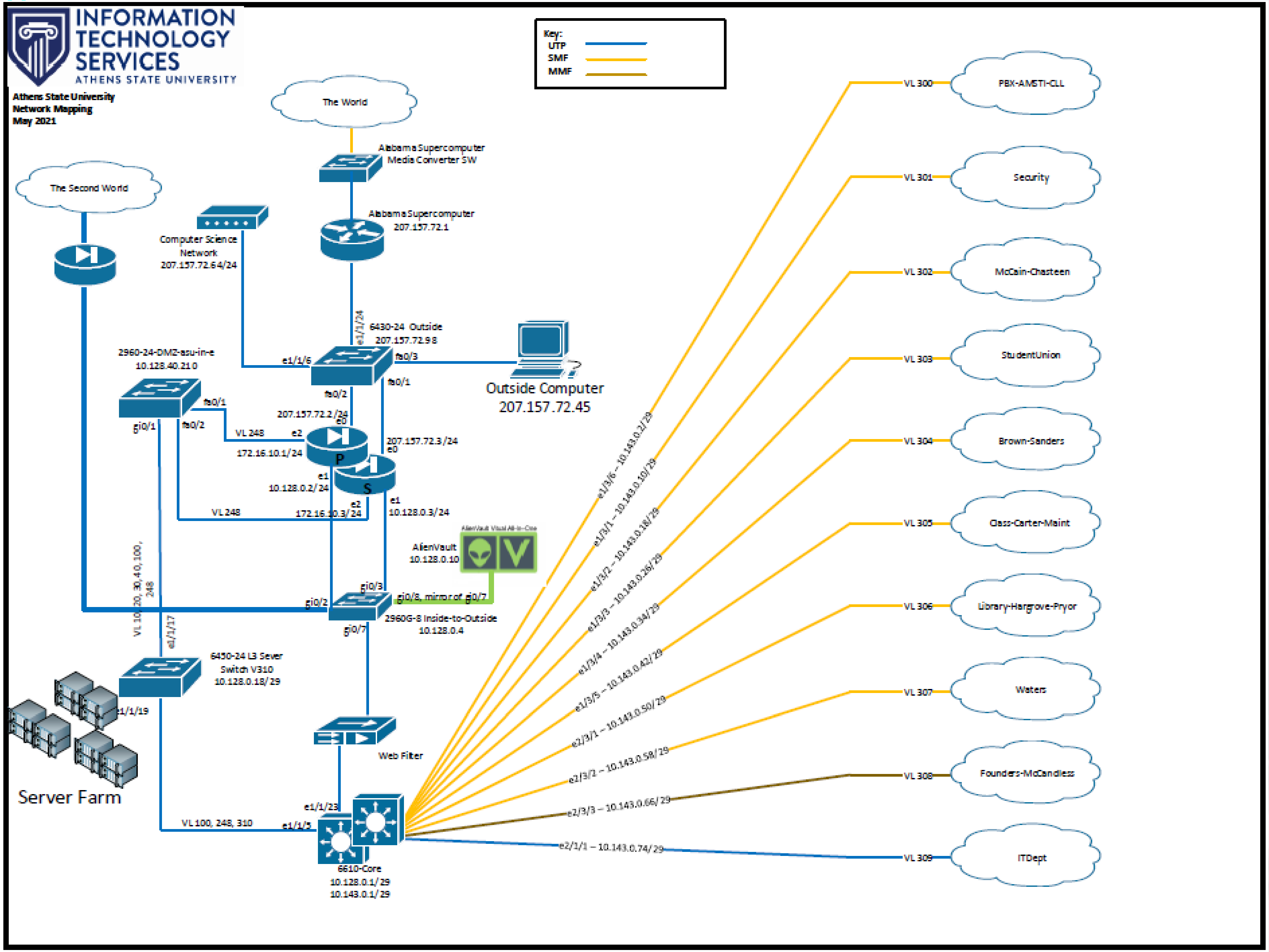
Redstone

Faculty/Staff Computers Classroom Workstations Student computer labs Library patron computers
Running Windows/Mac OS with Microsoft Office, Academic Software, Utilities, etc.

Updated: 2/7/2021

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

Athens State University
Network Mapping
May 2021



NETWORK SPRAWL

- 120 virtual servers:
  - 76 Linux based (ranging from other to Red Hat Linux 8)
  - 44 Windows Server based (ranging from 2008 R2 to 2019)
- Banner:
  - 40 in support of production Banner environment
  - 32 in support of the test and development Banner environment
- Windows:
  - 4 Domain controllers for main domain (athens.edu) and child domains (my.athens.edu)
  - 4 Exchange servers for faculty & staff
  - 1 network file share server
- 39 various security, application, and vendor specific servers

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

NETWORK & DATA ACCESS CONTROL

- Overlapping control of assets and access for convenience and expediency
- Too much access to network equipment rooms
- Inability to control what is being plugged into the network
- Granting access to resources based on ease vs actual need
    - Copying longtime employees' profile access for new employees
    - Granting access to non-departmental people for convenience
- Not removing access from people moving to different jobs, new departments, or leaving employment
- Not removing access or freedom of access (whitelists, access accounts, etc.) for venders/3rd party associates/and other non-university entities when no longer needed

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

CYBERSECURITY DEFENSE AND PROTECTION

- 4 firewalls
- 1 web security gateway
- 1 email security gateway
- 1 Security information and event management system (SIEM)
- 2 network stability systems (PSTV & SrvMon)
- End-point-protection
- 24/7 monitoring of all the systems, responding to ALL alerts, mitigating as necessary, resetting
- 3 people that wouldn’t recognize a whole day off if it bit them…

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

CYBERSECURITY DEFENSE AND PROTECTION

- Whitelists:
  - Firewall – 325 source exceptions coming in
  - Email SG – 182 source exceptions coming in
  - Web SG – 206 destination exceptions going out
- Blocks - well over 1,000,000,000 source and destination blocks:
  - Realtime blacklists
  - Shared information from FBI, EDUCAUSE-Security, HE-SRT, Homeland Security, REN-ISAC, and other sources
  - Observed malicious behavior by us

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

CYBERSECURITY DEFENSE AND PROTECTION

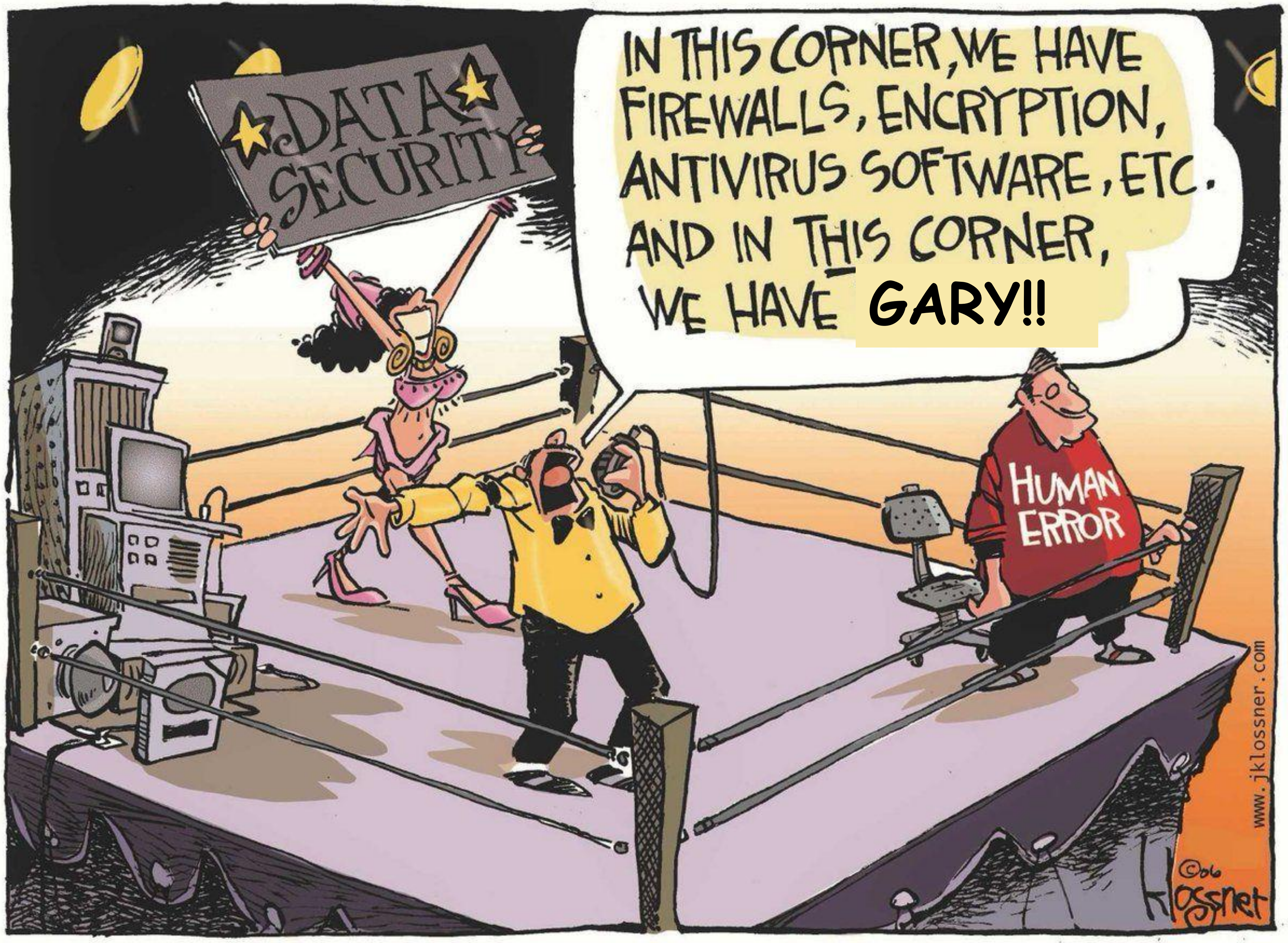
- Firewall for the first 12 days of July:
  - Advanced threat protection – scanned over 300,000 files
  - Intrusion prevention – processed over 93,000 events
- ALVA:
  - Monitoring over 1,400 devices
  - Processing over 300 events per second
- Alerts & notices:
  - ALVA – 602
  - Firewall – 1,225
  - O365 – 182
  - PSTV – 575
  - SPAM – 38
  - SrvMon - 778

INFORMATION
TECHNOLOGY
SERVICES
ATHENS STATE UNIVERSITY

CYBERSECURITY AWARENESS

Even if we had all the tools available on the market and a security staff to provide dedicated 24/7 coverage, we are still at the mercy of the biggest vulnerability…

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE GARY!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

Handout 1
Admin Council Minutes
July 2021
Page 24

OUR DEFENSE AGAINST GARY

- Defense in depth
- Only access and permissions necessary to do the job
- Periodic review of access
- Password complexity
- Frequent password changes
- Not using the same password
- Awareness

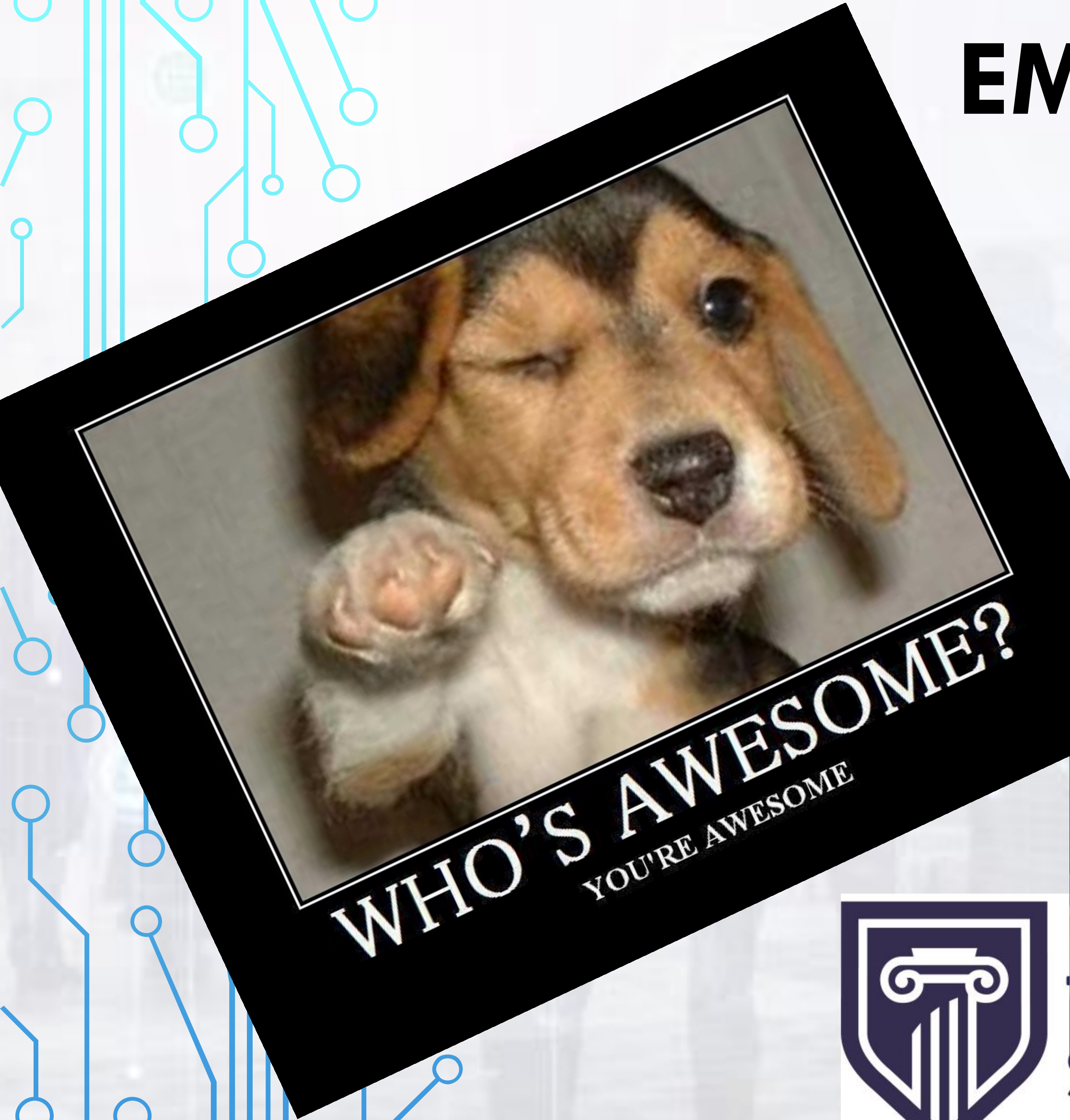
INFORMATION
TECHNOLOGY
SERVICES
ATHENS STATE UNIVERSITY

PASSWORD REQUIREMENTS

- Minimum characters – 13
- Must contain 3 of the 4:
  - 1 uppercase letter
  - 1 lowercase letter
  - 1 number
  - 1 special character
- No part of username
- Passwords cannot be reused until the fourth change/reset

INFORMATION
TECHNOLOGY
SERVICES
ATHENS STATE UNIVERSITY

A BIG SHOUT-OUT TO THE ATHENS STATE EMPLOYEES



SERVICES
ATHENS STATE UNIVERSITY

QUESTIONS?

INFORMATION
TECHNOLOGY
SERVICES
ATHENS STATE UNIVERSITY

BREAKOUT SESSION

INFORMATION TECHNOLOGY SERVICES
ATHENS STATE UNIVERSITY

Scenario Discussion Exercise

You work at public university. The country has been struck by a pandemic and the governor has issued an emergency order for non-essential state employees to stay home. Since it is mid-semester, all classes are being moved to online. Steps are taken to transition faculty and staff to work from home which relies heavily on technology to continue the university mission. In the midst of managing the pandemic, a ransomware attack occurs on campus. The campus network is not accessible, the telephone system (VoIP) is at the moment not working, and the Banner database has been encrypted by the ransomware and cannot be accessed. The ransom for unencrypting Banner database is $500,000 in Bitcoin.

Discussion questions

Does the campus have a viable continuity of operations plan or disaster recovery plan to use in response to the outlined scenario?

Does the campus have a plan for managing communications and processes without a computer system?

Do these plans make provisions for multiple threats occurring at the same time?

Does each department represented at your table have its own continuity of operations plan specific for responding to a technology failure? Is one needed? Is mission critical data used within the department residing on systems outside of Banner that is vulnerable to ransomware?

Does the campus need an Incident Response Plan that specifically details how to deal with a ransomware attack on mission critical systems?

What steps are required if there is no viable data backup to restore to bring the system back into operation without paying the ransom?

Should the organization have a plan in place for how to acquire Bitcoin?

Is the overall cost of restoring the technology resources to an operational level higher or lower than paying a ransom to restore the data? What is included in the cost of restoring the technology?

What core functions of the campus, dependent on technology, should be considered when developing a continuity of operations plan?

Can the core functions of the campus operate without technology?

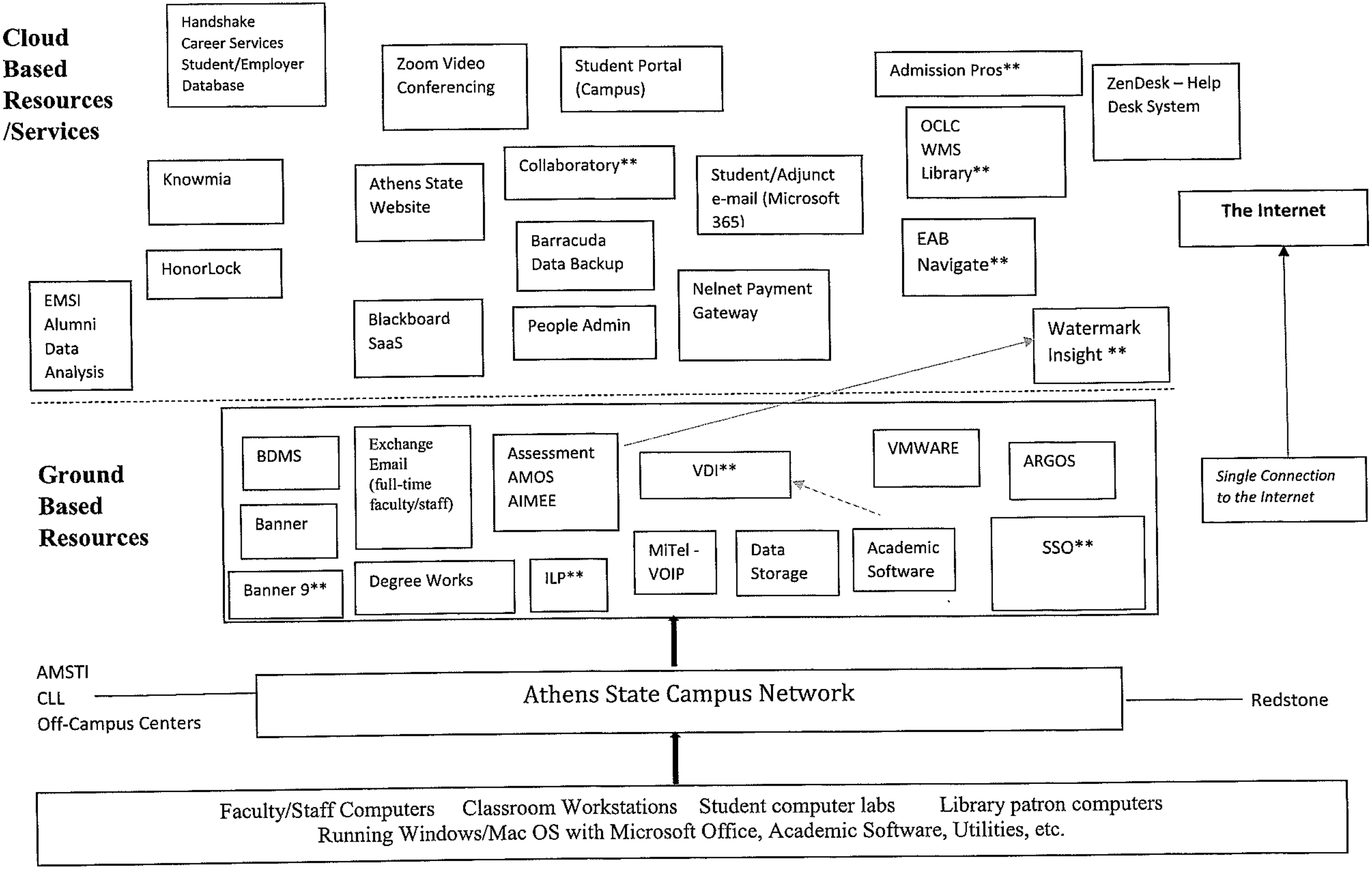
Are the dependencies on the current technology infrastructure of the campus creating a blind trust of IT's ability to restore technology to an operational level within an acceptable period of time?

Based on the discussions at your table, prepare a brief statement to share with the group in response to the following question:

Is a formal, technology failure/cyber-attack simulation exercise needed to determine gaps in current thinking that can be used to develop an incident response plan, continuity of operations plan, and disaster recovery plan for the university?

Athens State University Information, Communication, and Instructional Technologies - 2021

**Implemented since 1/1/2020.



Cloud Based Resources /Services

Handshake Career Services Student/Employer Database

Zoom Video Conferencing

Student Portal (Campus)

Admission Pros**

ZenDesk – Help Desk System

OCLC WMS Library**

Knowmia

Athens State Website

Collaboratory**

Student/Adjunct e-mail (Microsoft 365)

The Internet

Barracuda Data Backup

EAB Navigate**

HonorLock

EMSI Alumni Data Analysis

Nelnet Payment Gateway

Blackboard SaaS

People Admin

Watermark Insight **

Ground Based Resources

BDMS

Exchange Email (full-time faculty/staff)

Assessment AMOS AIMEE

VDI**

VMWARE

ARGOS

Single Connection to the Internet

Banner

MiTel - VOIP

Data Storage

Academic Software

SSO**

Banner 9**

Degree Works

ILP**

AMSTI
CLL
Off-Campus Centers

Athens State Campus Network

Redstone

Faculty/Staff Computers Classroom Workstations Student computer labs Library patron computers
Running Windows/Mac OS with Microsoft Office, Academic Software, Utilities, etc.

Updated: 2/7/2021