MAY UNIT REPORTS

HEALTH SCIENCES
CHIEF INFORMATION OFFICE

APPLICATIONS - RAY AVILA

SYSTEMS - PHIL MARQUEZ

SECURITY - MIKE MEYER

TECHNOLOGY SUPPORT - RICK ADCOCK

FOR MORE DETAILS:

Marcia Sletten, msletten@salud.unm.edu

APPLICATIONS TEAM

ACCOMPLISHMENTS

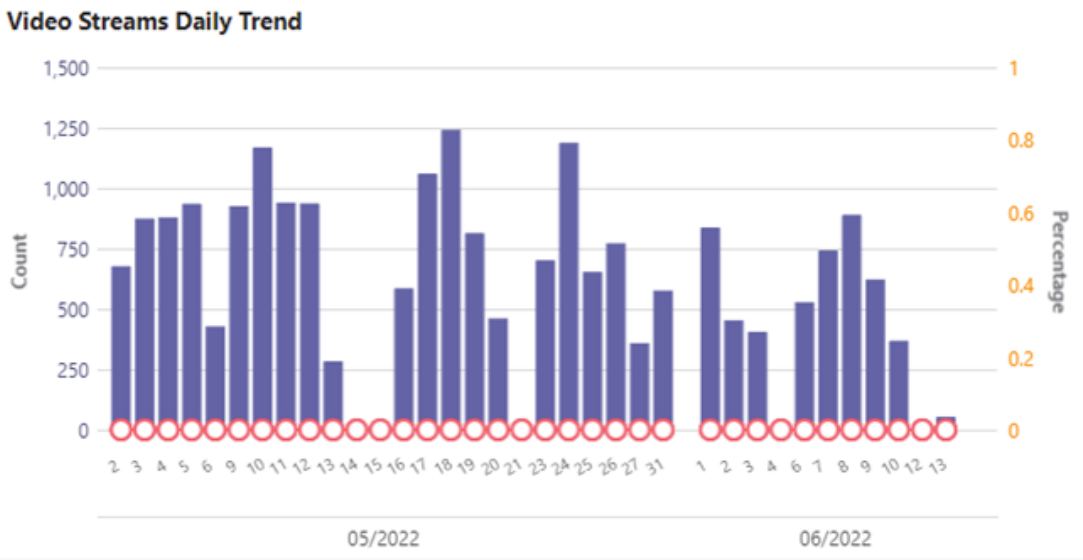
- Recreated 14+ legacy Learning Central Exams
- Implemented standard language, established passing scores and remediation requirements for HSC educational materials in Learning Central
- Finalized CTOC web app deployment preparation
- Launched the 2022 PA Supplemental Application application
- Closing of the FIBCI system and loading data to create FY23 in the SOM and CON/COP/COPH/HSLIC contract databases
- Updates to FACES and MDweb for the new curriculum year

IN-PROGRESS

- Zoom security enhancement
- M365 Intune implementation

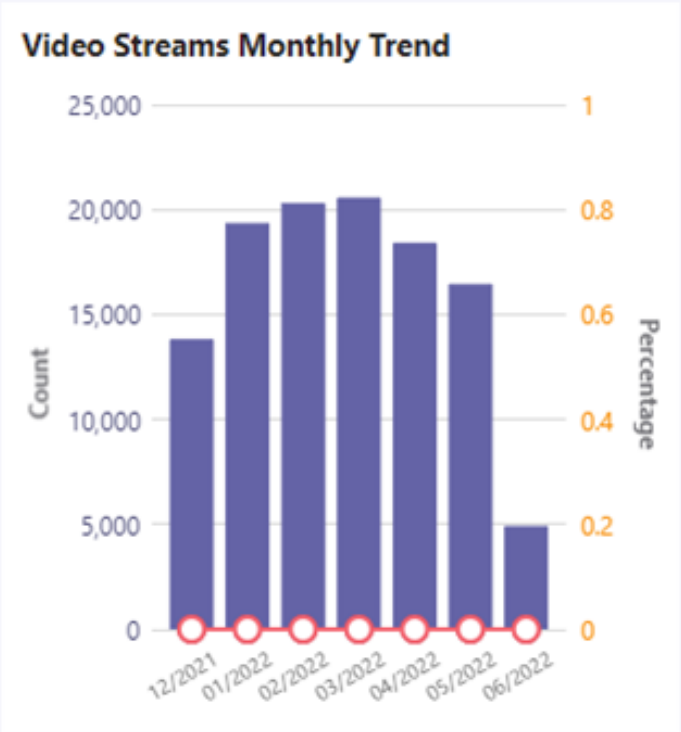
METRICS

- M365 Teams Usage

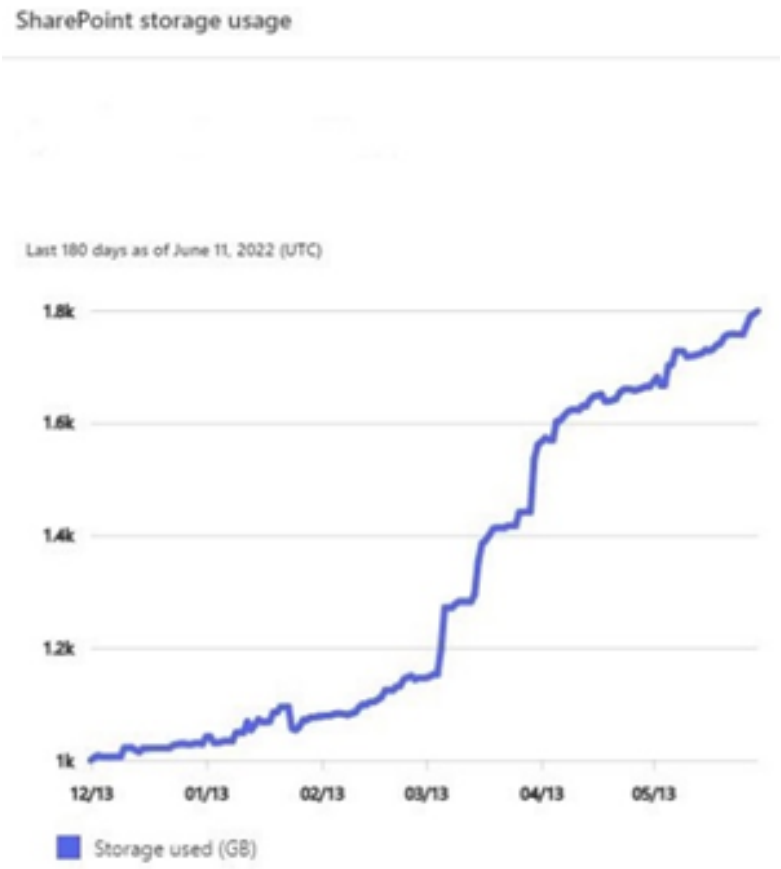


METRICS *(CONTINUED)*

- M365 Teams Usage

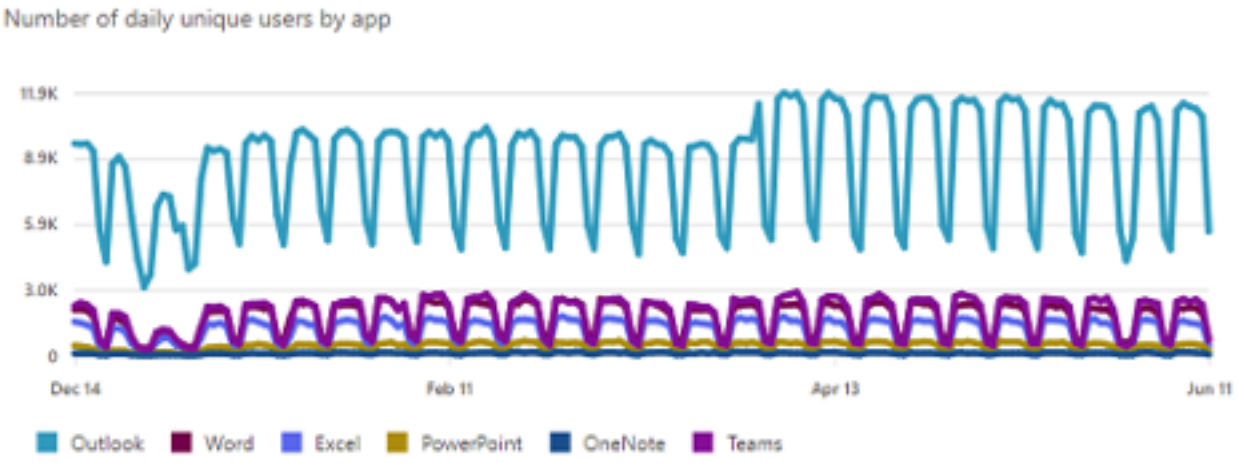


- M365 SharePoint Online (SPO)



METRICS *(CONTINUED)*

- M365 Application Usage



RECOGNITION

- I-Ching for having demonstrated persistence toward a creative and secure approach to Web Team Intranet needs.

SYSTEMS TEAM

ACCOMPLISHMENTS

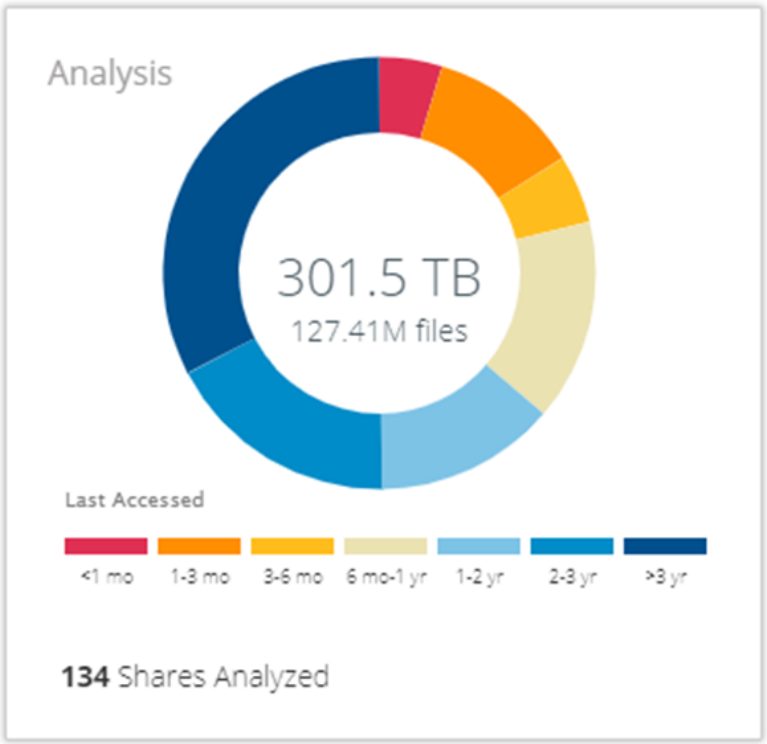
- No new major projects in March
- On Site Network Attached Storage replacement (Pure Storage)
  - Continued migrations of network folders from NetApp and Dell NAS (H:\Home, O:\ and N:\)
  - Reconciling folders exceeding number of allowed files in folders.
- Completed first monthly HSC Systems maintenance window on May 21 (7-9am)
  - F5 system upgrade
  - Rebooted HSC-HV01 to resolve a memory issue
  - Reconfigured HSC-WebApp1 virtual machine to increase drive space
  - No issues!
- Posted new position for Cloud Administrator in Systems team
  - Completed interviews, selected candidate.
  - Finalizing hiring process
- Completed NIH STRIDES Initiative sessions to simulate a research scenario
  - Excellent hands on learning opportunities in building out storage and virtual server environment within Azure as part of STRIDES POC for research.

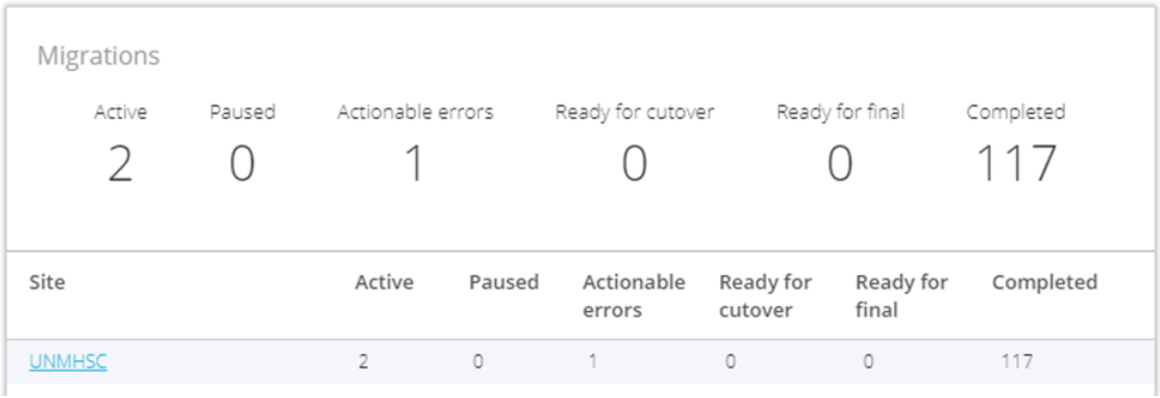
IN-PROGRESS

- Metallic cloud backup
  - Completed purchase of licenses for CDD data backup in Metallic
  - Still working to add licensing to provide Metallic backup for remaining unprotected data. All data on NetApp filers was retained with shadow copies, versioning, and replication. This will extend cloud backup and ransomware protection to include that data as well.
    - Pending resolution of move of data to cold storage solution
- Continuing data moves for \Homes: shared folders to Pure Storage
- Planning for June monthly maintenance window – 7/18/22 from 7-9am
  - Additional cut-over of \Homes: shares
  - Updates to PasswordState application

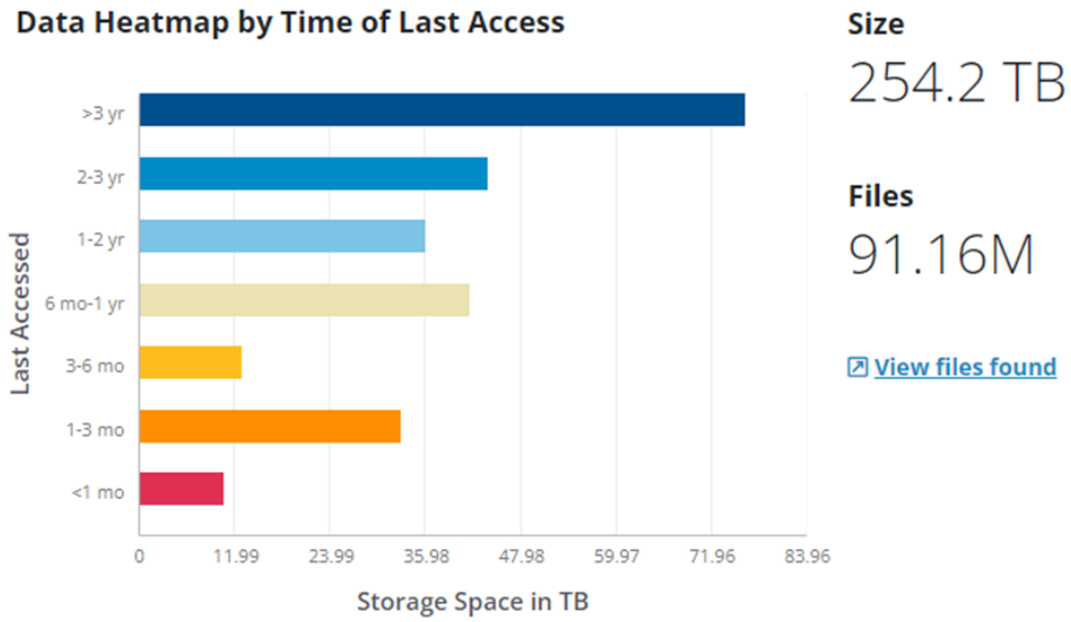
METRICS

- System availability:
  - No systems downtime
- Still working on completing standardized patching for domain controllers
  - Have not yet completed a full successful patch cycle without intervention
- This month's updates from Komprise Data Analysis tools showing graphs and metrics across all data stores
  - Aging reports showing data volumes by Last Accessed Dates
  - Ongoing Migrations
  - Space consumed by Top Shares





METRICS *(CONTINUED)*



RECOGNITION

- Joe Fresquez for efficiently completing IPRA and Legal email searches and providing excellent customer service to ensure results get delivered on a timely basis.

INFORMATION SECURITY OFFICE

ACCOMPLISHMENTS

ACCOMPLISHMENT	IMPACT
Executed statement of work with contractor (Optiv) to conduct an executive incident response exercise (ransomware) in early November. Held first planning meeting with Optiv.	Will provide executives insight into the dilemmas of ransomware attacks, particularly the “pay or not pay” paradox.
Participated in various training workshops on Azure implementation and security	The CIO has recognized that new tools and environment mean that IT staff must re-tool as well.
Network Security and ISO ran two phishing “challenges” in May.	Reducing successful phishing attempts reduces our risk exposure to ransomware attacks.

IN-PROGRESS

ACTIVITY	OBJECTIVE(S)
Implement Innovation Center Cyber Security using the U.S. government Cybersecurity Maturity	Conduct and document security reviews and establish security controls that are consistent and acceptable for the processing of ePHI in a cloud environment.
Improve Cyber Security Incident Response	Bring clarity to our incident response policy and plans. Provide "ransomware playbook” to speed response in the next incident. Conduct a major incident response in November 2022.

IN-PROGRESS (CONTINUED)

ACTIVITY	OBJECTIVE(S)
Improve Interior Security Controls	Implement additional security measures to limit lateral movement on our network if another attack penetrates our perimeter defenses.
Phishing Training	Conduct effective training in recognizing phishing attacks. Our target "click rate" is 5%. Current rate is around 30%.
Vulnerability Management	The goal of this effort for 2022 is to identify and begin to reduce our critical vulnerabilities. We have completed the first phase of this effort by successfully deploying a new product (Tenable.IO) to scan the entire network. Now the work is remediating the vulnerabilities found.
Protected DNS (pDNS) Collaboration with Main Campus	pDNS relies on threat intelligence to filter suspicious Internet addresses and is one of the major defenses against phishing, therefore ransomware. Collaboration with Main Campus will reduce overall cost for the service.

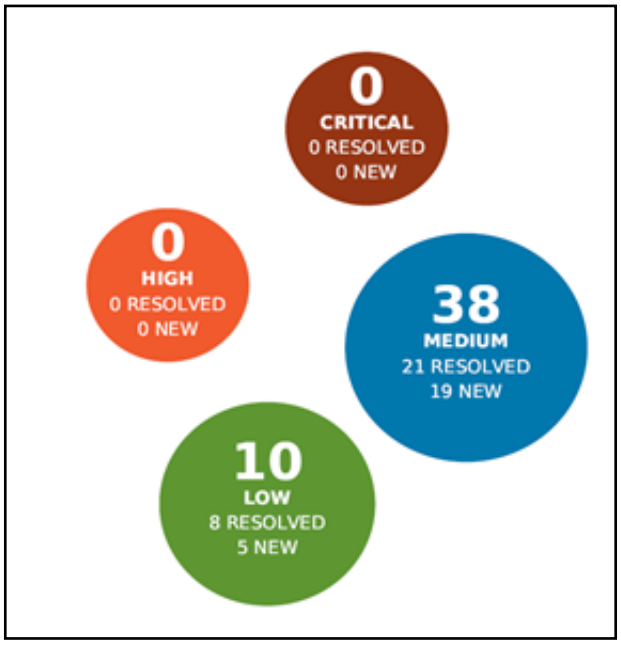
METRICS

Change requests	7 (1 urgent)
Certificate requests	1 new, 4 renewals
Software and Cloud service security reviews	20
Root Cause Analysis Submissions	0

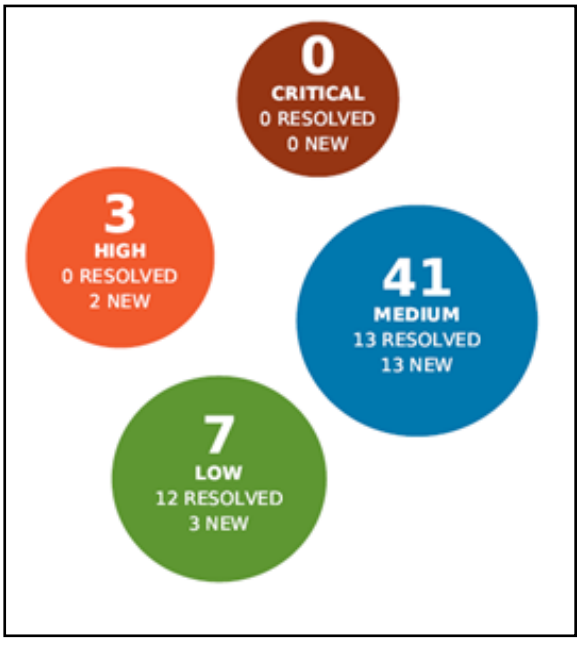
METRICS *(CONTINUED)*

DUA/SFTP Data Transfer Support Requests	28
Other Support Requests	48
Perimeter Vulnerabilities	Critical – 0 (No Change) High – 3 (Increase) Medium – 41 (Increase of 3) Low – 13 (Decrease of 3)
Enterprise Critical Vulnerabilities (entire network)	May = 65,678
Malicious email blocked by email firewall	15,155,881
Outbound email blocks for PHI content	144

Perimeter Vulnerabilities April 2022

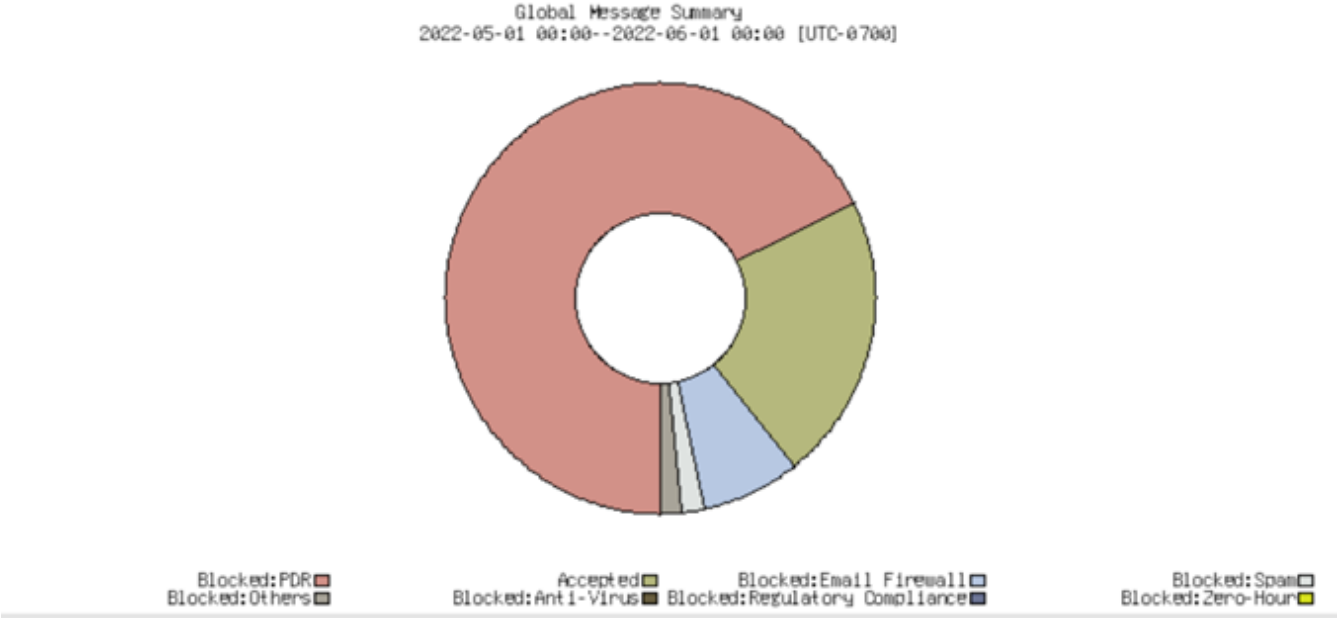


Perimeter Vulnerabilities May 2022



METRICS *(CONTINUED)*

ProofPoint Email Defense May 2022

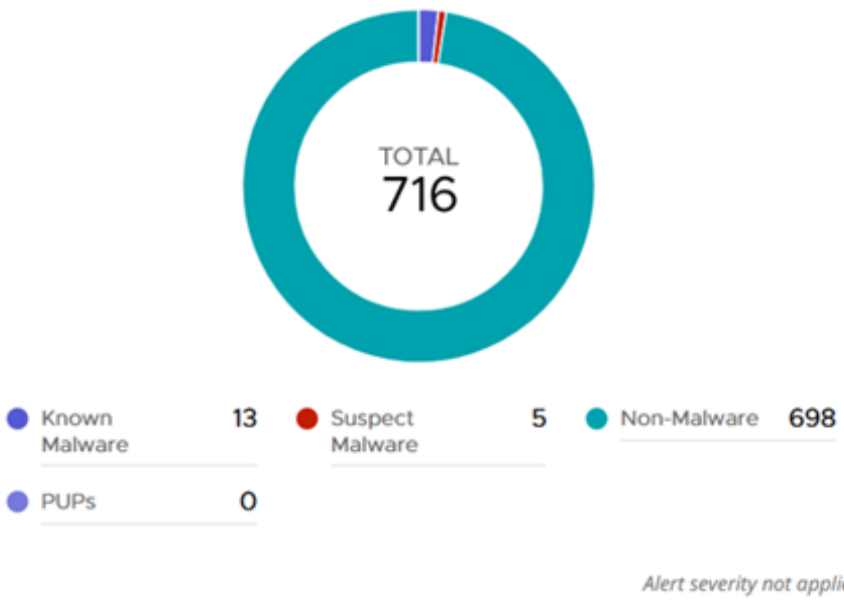


ProofPoint Messages Processed and Rejected

Type	Messages	Percent
Blocked:PDR	13081605	67.74%
Accepted	4155163	21.51%
Blocked:Email Firewall	1442856	7.47%
Blocked:Spam	331524	1.71%
Blocked:Others	295842	1.53%
Blocked:Anti-Virus	3846	0.01%
Blocked:Regulatory Compliance	144	0%
Blocked:Zero-Hour	64	0%
Total	19311044	100%

Notes: PDR = Proofpoint Dynamic Reputation service “Regulatory Compliance” = Outbound email containing ePHI not properly encrypted

Carbon Black Endpoint Detection and Recovery - Blocked Attacks



TECHNOLOGY SUPPORT

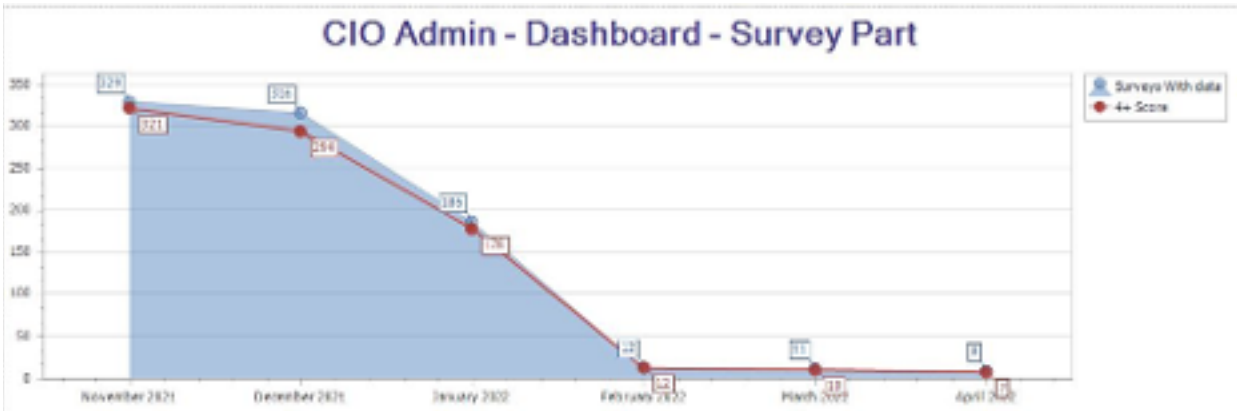
ACCOMPLISHMENTS

- Released the new Dell OptiPlex 7000 Workstation in LoboMart
- Remediated UH Domain Admin accounts to move forward with utilizing pass phrases in lieu of passwords on HSC accounts
- Released a new Windows 10 Gold Image for the institution

IN-PROGRESS

- Remediation of unencrypted workstations
- Intune configuration for enrollment and workstation management
  - Intune for OSX enrollment process in Apple School Manager, and management configuration
  - Windows Patching
  - Compliance Reporting
- Password Policy re-design for pass phrases
- Using NoMad for AD bind issue of OSX devices
- Testing Softphones for off-site access to the Automated Call Distribution system

METRICS



METRICS *(CONTINUED)*

Current Workstation Encryption Status