MARCH UNIT REPORTS

HEALTH SCIENCES
CHIEF INFORMATION OFFICE

APPLICATIONS - RAY AVILA

SYSTEMS - PHIL MARQUEZ

SECURITY - MIKE MEYER

TECHNOLOGY SUPPORT - RICK ADCOCK

NM OFFICE OF THE MEDICAL INVESTIGATOR - MARTIN WETTERSTROM

FOR MORE DETAILS:

Marcia Sletten, msletten@salud.unm.edu

APPLICATIONS TEAM

ACCOMPLISHMENTS

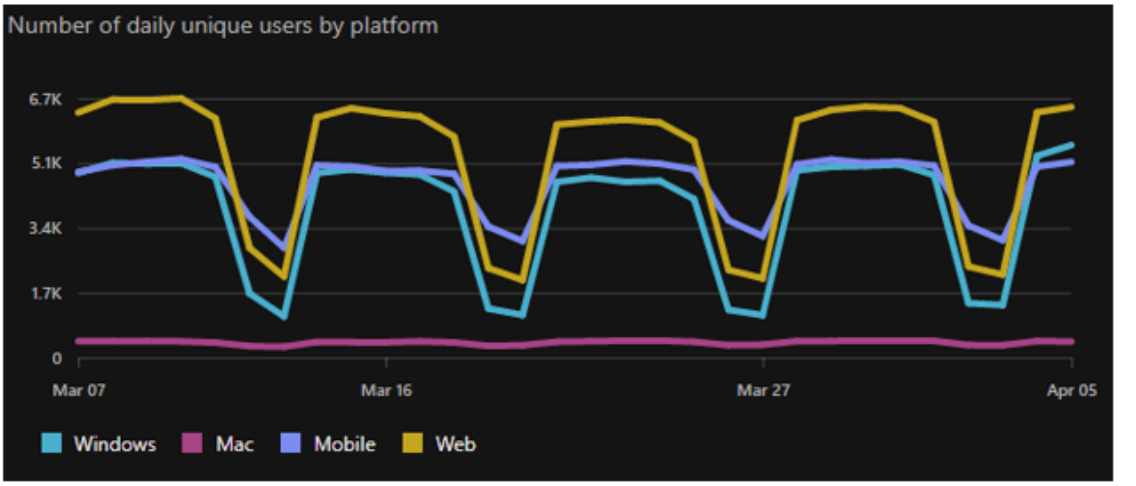
- Successfully sunset SharePoint 2010 environment
  - >130 sites
  - Dozens of site owner consultations
  - Significant outreach efforts to individual site owners and HSC
  - Dozens of migrations
- Launched FY23 FIBCI and salary increase database setup for all HSC Colleges
- Launched Intune Kickoff for HSC M365
- Provisioned 80 new Zoom licenses

IN-PROGRESS

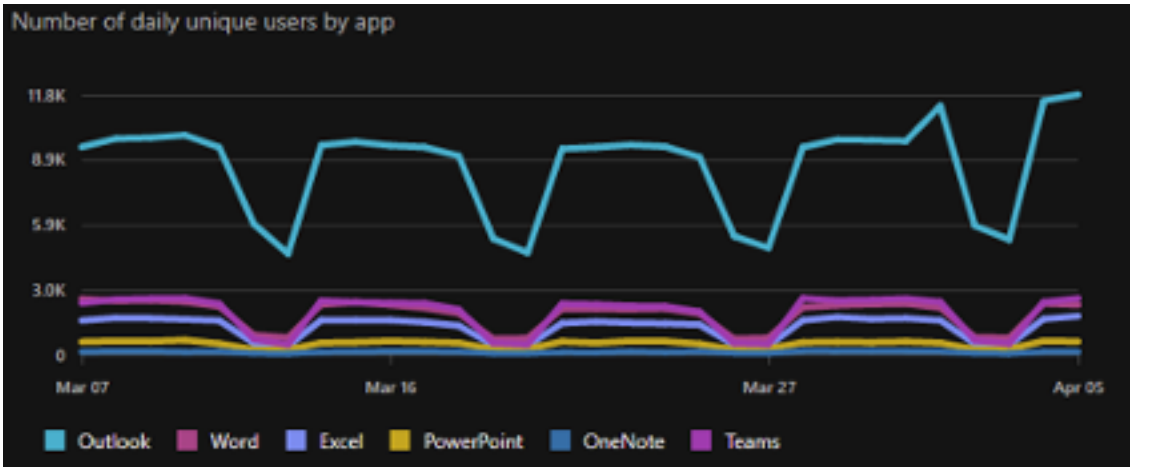
- Zoom Security Enhancement
- M365 Intune Implementation

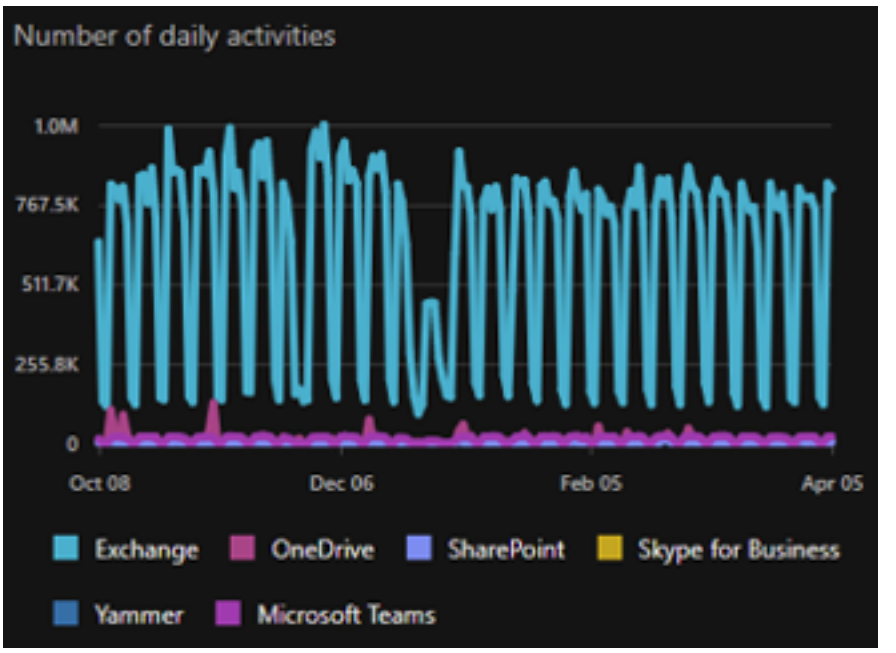
METRICS

M365 Usage:



METRICS *(CONTINUED)*





RECOGNITION

- Corey Payton for his extensive efforts surrounding the SharePoint 2010 sunset initiative. He provided superior customer service, outreach, and technical work that resulted in a significant environment being retired from our HSC. He was able to do so while maintaining strong support and maintenance to our HSC cloud services.

SYSTEMS TEAM

ACCOMPLISHMENTS

- No new major projects in March
- Completed Performance reviews for the team
- On Site Network Attached Storage replacement (Pure Storage)
  - On Site Network Attached Storage replacement (H:\Home, O:\ and N:\ network shares)
  - Completed installation week of March 11.
  - Configuring Komprise migration tool to move existing data to new storage appliance

IN-PROGRESS

- Attending NIH STRIDES Initiative sessions to simulate a research scenario
- Metallic cloud backup
  - Working with vendor on quotes to extend Metallic backup service to CDD servers and virtual machines
- Working with Nutanix engineers to add capacity to on-site high availability cluster to host VMs
- Working with Pure Storage and Komprise to provide migration and replication services to multiple on-site storage devices
  - This will provide a second on-site copy of network data shares
- Began investigating redundant cooling options for BRF data center
  - The current HVAC system is a single point of failure for the data center
  - We are investigating options to provide a backup cooling solution

METRICS

- System availability:
  - BRF Uninterruptible Power System (UPS) #2 unexpectedly tripped a breaker during a power failure on the evening of 3/3/2022. Power was lost and the backup power came on as expected, but normally half the systems receive primary power through UPS2. Since the breaker tripped on UPS2, all systems were powered through UPS1.
    - A very small number of devices only have a single power source and were down throughout the power outage.
      - Monitoring system and
- Still finalizing a standard monthly maintenance window
- Still working on completing standardized patching for domain controllers
  - Issues with SCCM being worked with Microsoft
- We will have full access to Komprise Data Analysis tools in the next month or so to be able to produce data use graphs and other metrics

RECOGNITION

- Joe Fresquez for efficiently processing a high number of IPRA email searches through e-Discovery

INFORMATION SECURITY OFFICE

ACCOMPLISHMENTS

ACCOMPLISHMENT	IMPACT
Geoff Johnson accepted our offer to fill the Security Operations Manager position in the ISO.	At full staff again, the ISO will be more effective in guiding HSC toward a more unified, enterprise security posture.
Entire ISO team participated in Planet Technology training on using and securing Azure infrastructure as part of Innovation Center/STRIDES project	May provide new AI and ML tools to improve tools available for HSC researchers.
Participated in Tenable "Quick Start" training for implementation of Tenable.IO	Tenable.IO is our replacement vulnerability scanner. We are now scanning our public-facing systems daily and alerting on any new critical or high vulnerability. We are now scanning the entire network regardless of department monthly, with the goal of scanning weekly in line with best practices and cyber insurance carrier requirements.
ISO team participated with UH Network Security and UH Cyber Security in a threat hunting exercise sponsored by one of our vendors.	Threat hunting in the cyber world involves searching and understanding security logs. This was excellent training that will improve our team's ability to recognize threat activity and respond more quickly in the event of a future ransomware attack.

IN-PROGRESS

ACTIVITY	OBJECTIVE(S)
Implement Innovation Center Cyber Security using the U.S. government Cybersecurity Maturity Model Certification (CMMC) standards.	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 clarify to our incident response policy and plans. Provide "ransomware playbook" to speed response in the next incident. Conduct a major incident response in Oct 2022.
Improve Interior Security Controls	Implement additional security measures to limit lateral movement on our network in the event that 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.

METRICS

Change Requests	7
Certificate requests	4
Root Cause Analysis submissions	3
Software and Cloud service security reviews	25
DUA/SFTP Data Transfer Support Requests	23
Perimeter Vulnerabilities	Critical – 0 (No Change) High – 0 (Decrease) Medium – 38 (Increase) Low – 16 (Increase)
Enterprise Critical Vulnerabilities (entire network	23,453 (First time reporting)
Malicious email blocked by email firewall	31,483

Phishing Challenge Results to Date

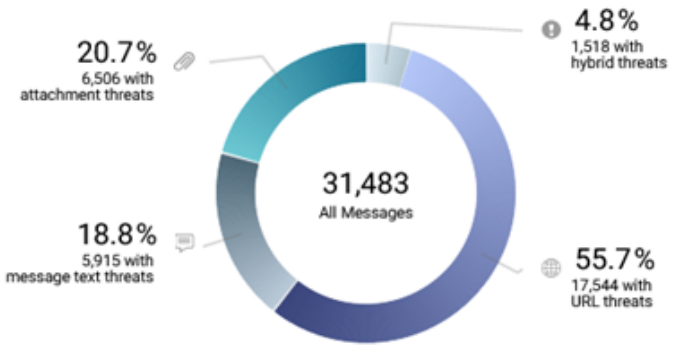
Goal is <5% Click Rate (Number who clicked phishing link / Number who read the message)

MONTH	TOPIC	# OPENED	CLICKRATE	REPORT RATE
Jan 2022	HIPAA	2732	34%	20%
Jan 2022	Netflix	1182	11%	23%
Feb 2022	Turbo Tax	9118	1.9%	6.2%
Feb 2022	Teams	12264	17%	12%
Mar 2022	EMR	9281	24%	12%

METRICS *(CONTINUED)*

Perimeter Vulnerabilities

Email Threat Types by Volume



RECOGNITION

- Meghann Carrillo in Network Security. Meghann saw a training opportunity to participate in a threat hunting lab event using the vendor's capability. Meghann coordinated this event to optimize participation. Threat hunting is one of our weak areas. We do not have enough analysts trained in this. Meghann's efforts helped move us in the right direction.

TECHNOLOGY SUPPORT

ACCOMPLISHMENTS

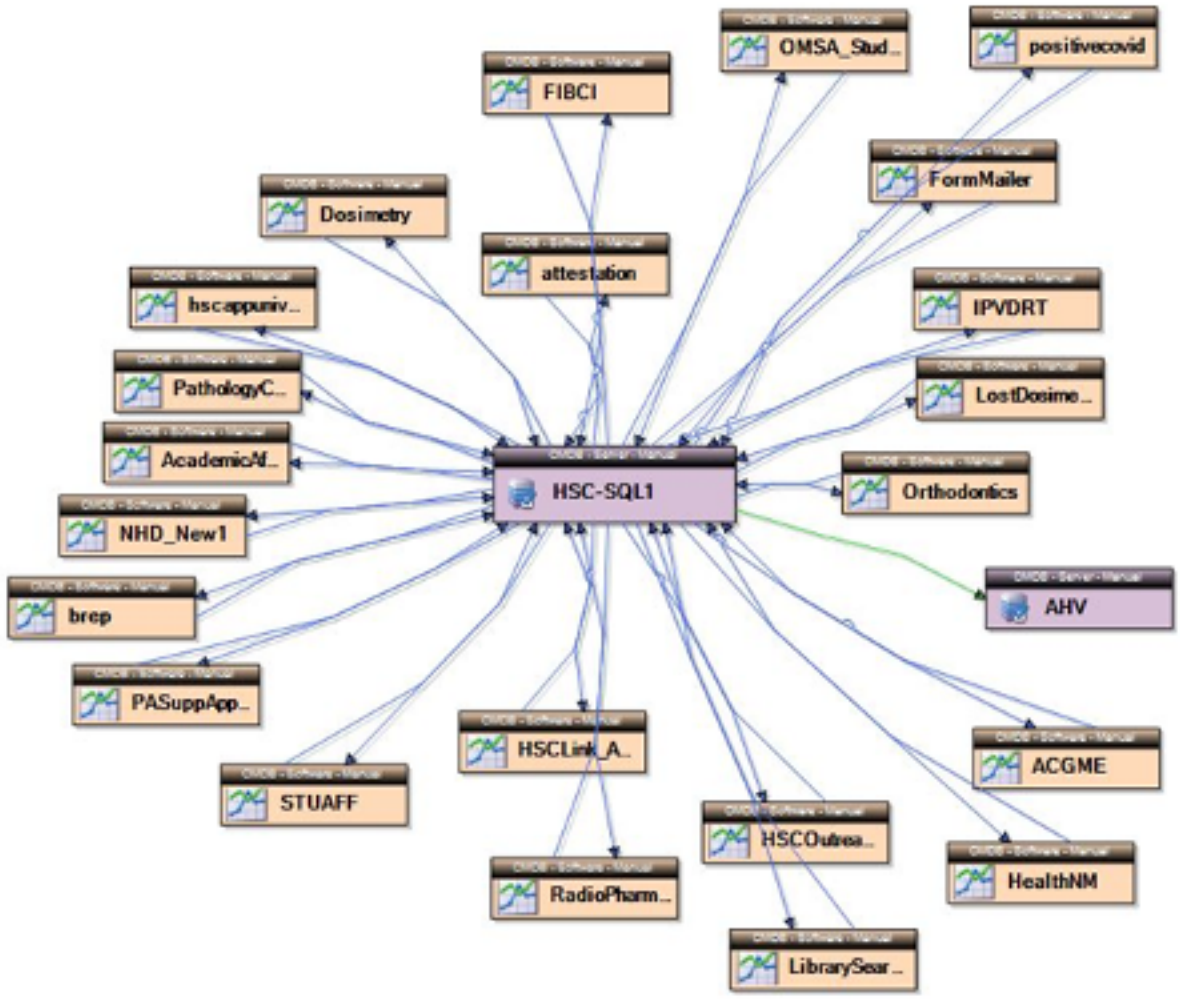
- Completed Microsoft Intune training
- Release the new Windows 10 workstation image
- Facilitated meeting with Planet Technologies and Project Echo to work on the move from Box.com to MS365
- Presented the HSC configuration management database (CMDB) and visualizations to IT Managers

IN-PROGRESS

- Remediation of unencrypted workstations
  - Departmental IT staff remediating their workstation
  - HSC IT staff remediating the remaining workstations
- Preparing for the new Dell Laptop and Desktop models
  - Update standard quotes
  - Change standard configurations in Lobomart
- Creating new monitoring station for services (Network bandwidth, etc.)

METRICS

CMDB Visualization



RECOGNITION

- Aaron Douglas had his position reclassified to a Core IT Services Specialist. Well deserved!

NM OFFICE OF THE MEDICAL INVESTIGATOR

ACCOMPLISHMENTS

- FEMA DMORT Visit
  - 10 people stationed at OMI for 2 weeks.
  - Assisted with searching for and locating next of kin.
  - Significant reduction in storage of unclaimed/indigent decedents.
- Case Management System (CME)
  - Phase II A, B and C releases completed.
  - Formed a review team, consisting of at least one team member from every area or department. All members are heavy application users, with process knowledge of their department.
  - Implemented an SBAR process for future change requests in the application.
  - Finalized turnaround time reports for the pathologists.
  - Daily reports going out to Bernalillo County with Bernalillo County unclaimed/indigent decedents.
  - Listing on OMI's web site of decedents without next of kin identified.

IN-PROGRESS

- Case Management System (CME)
  - Phase III A items currently in review with the review team.
  - Process change for investigator, utilizing MS Teams while out in the field.
  - Phases III B and C, phase IV and phase V.
  - Integration with BVS DAVE system.
  - Sunset of the legacy applications.

RECOGNITION

- Mike Garcia and Marc Leasure for getting the DMORT team up and running.
- Lewis Worley for assisting with reports.
- All of the IT departments for scrambling and finding PC's and getting networking setup for the DMORT team.