405(d) Spotlight Webinar

Monitoring and Responding to Cyber Threats: A Look into FDA's role in monitoring threats and how one CISO is responding and protecting his Organization

Jessica Wilkerson, Cyber Policy Advisor (FDA/CDRH/OST/ARC)
Dan Bowden, VP & CISO, Sentara Healthcare

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) Task Group member; each iteration does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute this webinar series.

* This Webinar is being recorded and will be available for future viewing

405(d) Events and Announcements

- **May**
  - Continuation of 405(d) Spring Campaign
  - 405(d) Post 5/20
  - State Healthcare IT Connect Summit 5/20
- **June**
  - Continuation of 405(d) Spring Campaign
  - Spotlight Webinar- Date TBD
- **July**
  - Continuation of 405(d) Spring Campaign
  - 405(d) Post 7/22

Agenda

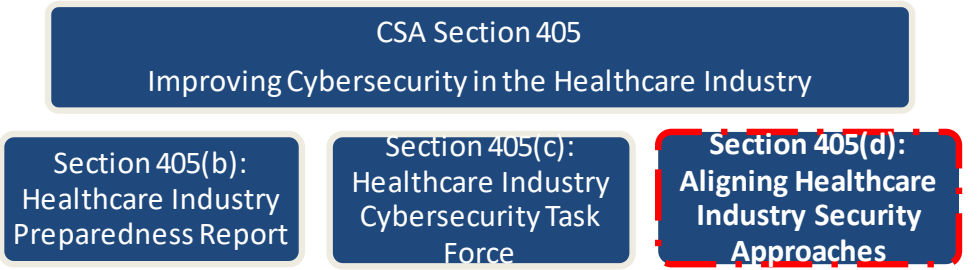
Time	Topic	Speaker
10 minutes	Opening Remarks and Introductions	Julie Chua, HHS
10 Minutes	FDA Monitoring and Responding to Cyber Threats	Jessica Wilkerson
10 Minutes	Industry Response to Recent Threats	Dan Bowden
20 Minutes	Panel Discussion	All
10 Minutes	Q&A and Closing	All

Cybersecurity Act of 2015: Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of "Aligning Health Industry Security Approaches" by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !



405(d) Resources

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released over 50 awareness products which organizations across the HPH sector can leverage

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters, The 405(d) Post, and Spotlight Webinars to increase cybersecurity awareness and present on new and emerging cybersecurity news and topics, as well highlighting the HICP Publication!

405(d) Social Media

The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

NEW RESOURCES ALERT

405(d) "That Seems Risky" Campaign

405(d) Cybersecurity "Myth vs. Fact" Campaign

Jessica Wilkerson

Jessica Wilkerson is a Cyber Policy Advisor with the All-Hazards Readiness, Response, and Cybersecurity (ARC) team in the Center for Devices and Radiological Health (CDRH) within the Food and Drug Administration (FDA). As part of ARC, she examines issues and develops policy related to the safety and effectiveness of connected medical devices. She received a B.A. in Policy Studies and minors in Computer Science and Mathematics from Syracuse University, and is currently pursuing a J.D. from the Catholic University of America's Columbus School of Law.

Dan Bowden

Dan Bowden is Chief Information Security Officer for Sentara Healthcare.
Over the past 30 years, he has been a cybersecurity leader in healthcare, higher education, banking, retail, and the military.
He also represents Sentara's interests in blockchain consortiums and networks directed at the goal of improving healthcare services and cost.
He has been active with various HSCC-CWG, and 405(d) efforts the past five years.
His education includes a Master's Degree in Administration of Justice and Security with a Concentration on Global and Homeland Security.

FDA Cybersecurity Work

Jessica Wilkerson
Cyber Policy Advisor
FDA
CDRH/OST/DARSS/ARC

The FDA is responsible for ensuring that medical devices are designed to provide "reasonable assurances of safety and effectiveness" before they may be marketed to patients and consumers.

Why does this matter when it comes to cybersecurity?

Because **Cybersecurity** is a **Patient Safety Issue**

FDA has found 510(k) submissions to be "not substantially equivalent" (NSE) and "postmarket approval" (PMA) devices to be not approvable based on cybersecurity concerns alone.

2014-2020: What Have We Learned?

- Sector is maturing to be able to consider risks throughout the product lifecycle to better acknowledge and respond to reality that cybersecurity risks can arise at any time.
- Additional information about software design decisions and software supply chain would increase ability of agency/manufacturers/others to better contextualize risks.
- “Building in” rather than “bolting on” security is more effective and efficient.
- Evaluation of security controls in more realistic contexts ensures more effective implementation. Stakeholders would benefit from more and better information about how to manage risks.
- Managing cybersecurity risks goes beyond simply security controls in devices—organizational infrastructure (such as CVD programs) are needed as well.

How FDA Responds to Cybersecurity Vulnerabilities

- In addition to ensuring that medical devices provide "reasonable assurance of safety and effectiveness" before they may be marketed, FDA is also responsible for ensuring such devices <u>remain safe and effective</u> once on the market.
- If an issue—cybersecurity or otherwise—is discovered in a medical device, the FDA takes action to:
  - Evaluate the risk of patient harm as a result of the vulnerability
  - Collaborate with other appropriate parties (including the manufacturer of the device) to develop mitigations or "fixes"
  - Where appropriate, inform the public of the vulnerabilities.

INFORMATION SECURITY
Cyber-Threat Response
4/23/2021

Dan Bowden
Chief Information Security Officer for Sentara Healthcare

Protect-Detect-Respond

Controls Mitigating Threat Exposure:

- Cyber Threat Intelligence
- Email Security Appliance
- Web Security Appliance
- Endpoint Protection
- Umbrella Domain Name Services Security
- Tool Instrumentation
- Privileged Access Management
- Duo 2FA
- Network Segmentation
- Vulnerability Compliance Management
- Patching & Virtual Patching
- Web App Shielding
- Weekly Vulnerability Scans
- Penetration Testing
- Malware Analysis and Response – SPAM Mailbox
- On Premise Malware Sandbox
- Medical Device Security Platform

Awareness and Training

- Monthly Phishing Campaigns
- Corporate Communications
- Annual regulatory OneLink learning
- National Cyber Security Awareness Month (NCSAM)
- Cybersecurity Training Resource Wavenet Page
- Education - Workplace by Facebook

Recommendations

- Blocking consumer email
- Web isolation
- Increased awareness and training efforts
- Limited email and web access

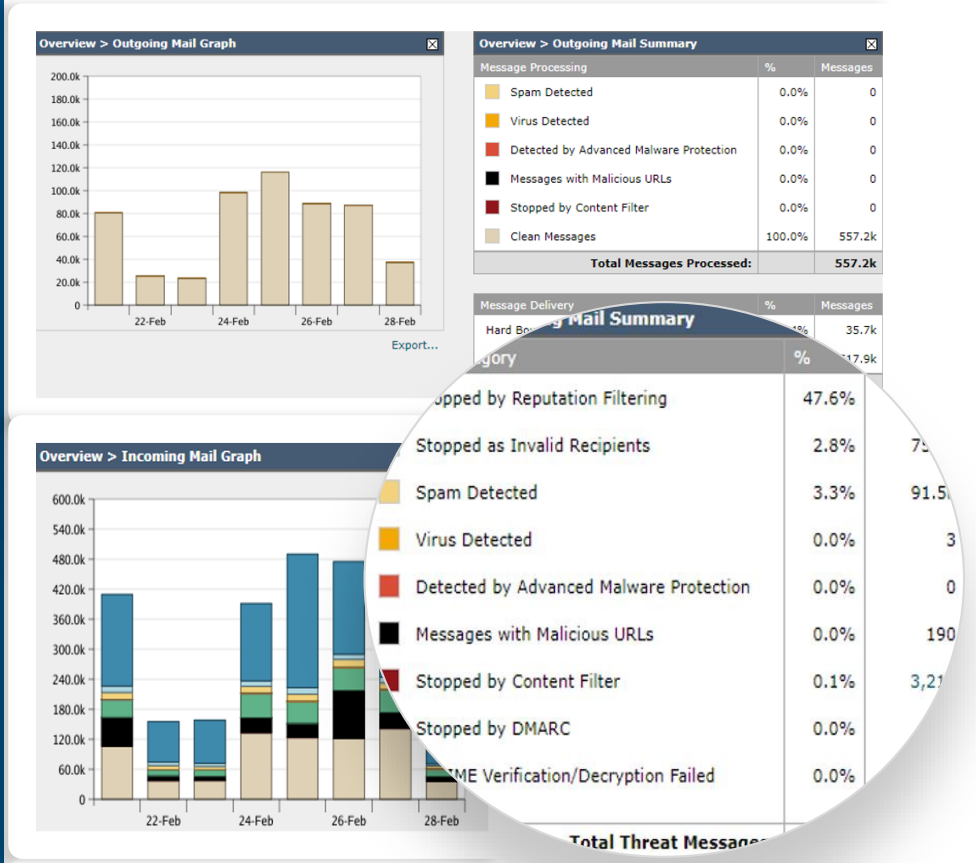
Controls Mitigating Threat Exposure

Cyber Threat Intel -- Ingest

We ingest, evaluate, and act on threat intelligence from multiple sources:

- **IBM Xforce** | Provides enrichment to SIEM data
- **ISAO** | Weekly calls to share current threats and vulnerabilities among similar healthcare organizations.
- **NH-ISAC** | Healthcare specific threats
- **FlashPoint**| Deep Dark Web News & Threats/Compromised Credential notification/Sentara key work alerts
- **PasteBin** |Sentara keyword and IP Range alerts
- **TruStar** | Threat Intelligence Platform. Utilized by ISAO for automated threat sharing
- **MarkMonitor** | Domain name monitoring
- **CISCO Talos** | Incidence and Response Specialists

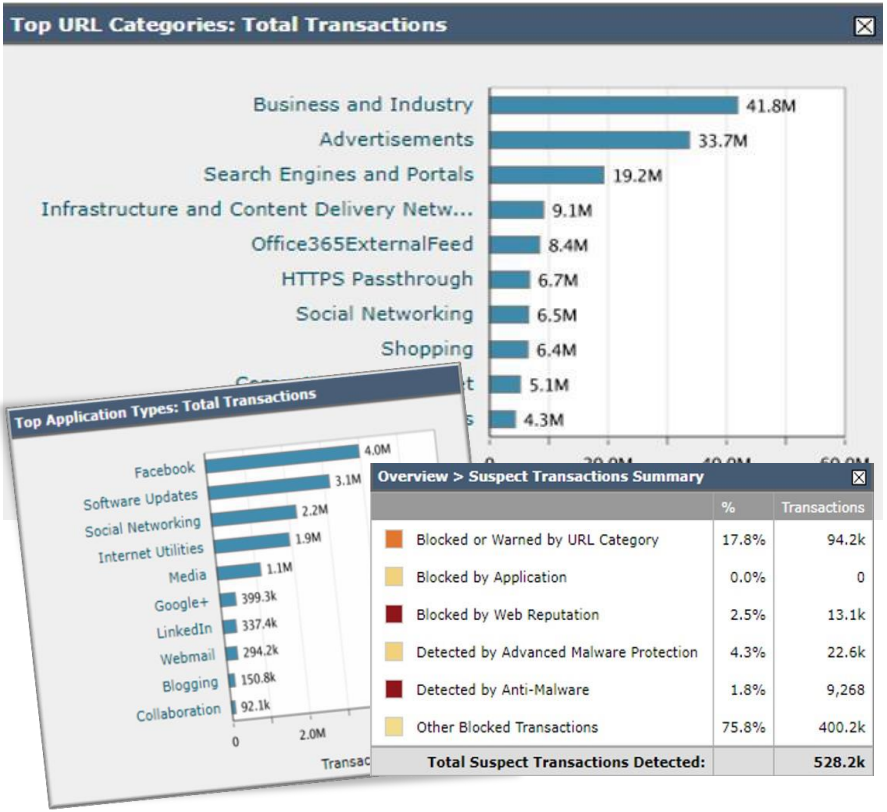
Email Security Appliance



ESA Overview:

- Monitors all incoming and outgoing mail
- Uses dynamic threat intelligence
- Inspects attachments and links
- Quarantines spam content and blocks malicious content

Web Security Appliance



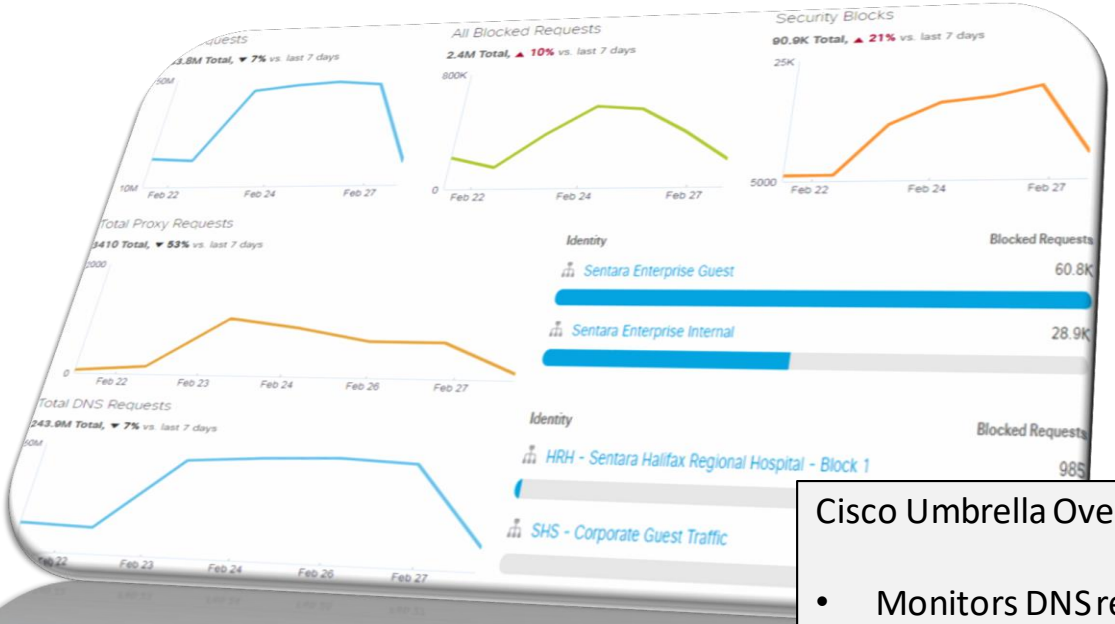
WSA Overview:

- Monitors all web traffic
- Uses dynamic threat intelligence
- Blocks malicious or inappropriate content based on category filtering
- Monitors high bandwidth users

Anti-Virus Endpoint Protection

- Anti - Virus protection (A/V) linked to QRadar SIEM, and Cisco ISE
- Status of devices and success of removal centrally managed

Cisco Umbrella Domain Name Services Filtering



Cisco Umbrella Overview:

- Monitors DNS requests
- Blocks requests based on dynamic destination lists and defined policies

Security Instrumentation Platform (Verodin)

SIP enables us to understand and communicate Cyber security effectiveness with quantifiable, evidence-based data

Controls Effectiveness

- Test, challenge and validate controls effectiveness and configuration assurance

Optimization

- Identify gaps in security effectiveness due to equipment misconfiguration, evolving attacker tactics and changes in the IT environment

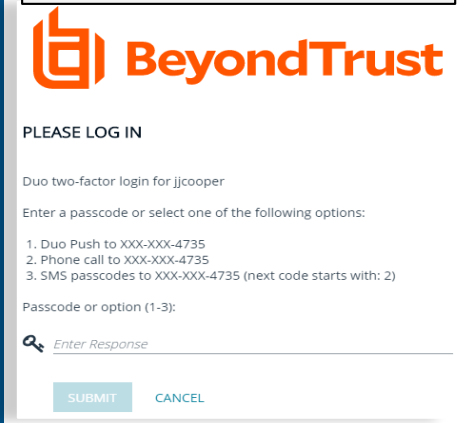
Automated Environmental Drift Detection

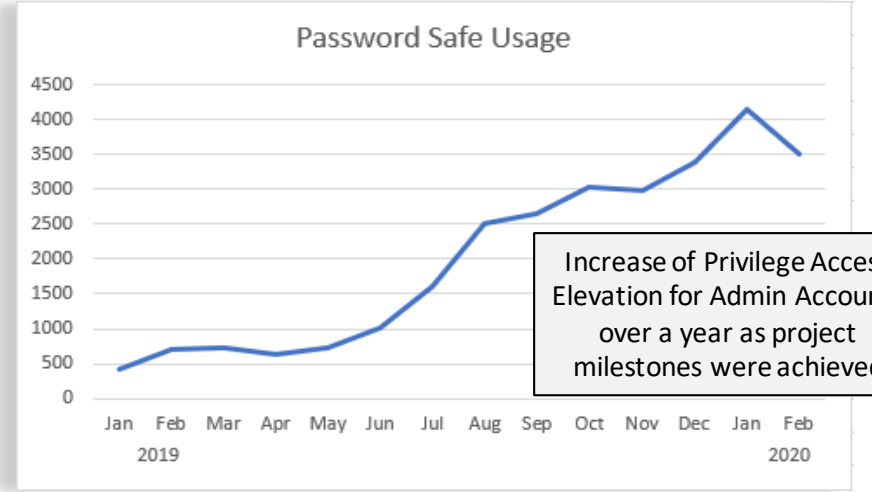
Rationalization

- Rationalize cyber security spend by identifying and removing overlapping controls

Privileged Access Management

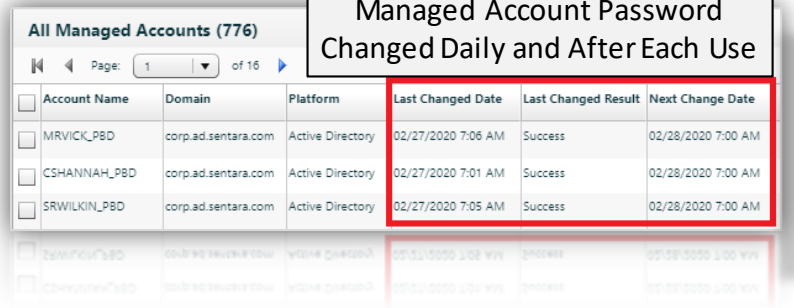
Duo MFA Required at Login





Increase of Privilege Access Elevation for Admin Accounts over a year as project milestones were achieved

Managed Account Password Changed Daily and After Each Use

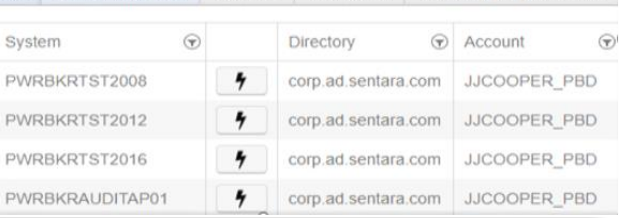


All Managed Accounts (776)

Page: 1 of 16

Account Name	Domain	Platform	Last Changed Date	Last Changed Result	Next Change Date
MRVICK_PBD	corp.ad.sentara.com	Active Directory	02/27/2020 7:06 AM	Success	02/28/2020 7:00 AM
CSHANNAH_PBD	corp.ad.sentara.com	Active Directory	02/27/2020 7:01 AM	Success	02/28/2020 7:00 AM
SRWILKIN_PBD	corp.ad.sentara.com	Active Directory	02/27/2020 7:05 AM	Success	02/28/2020 7:00 AM

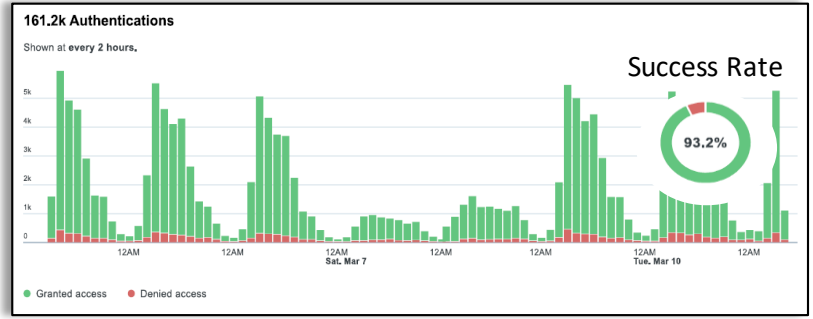
Servers and Privileged Accounts are Displayed

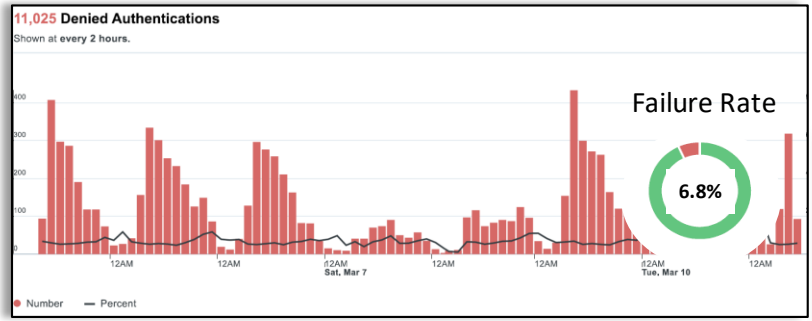


ites | Recently Used | Systems | Databases | Domain Linked Accounts

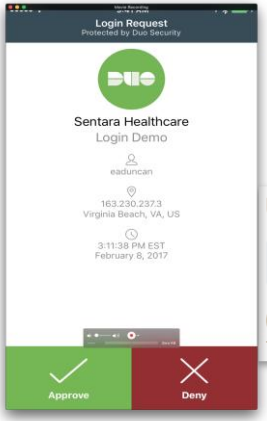
System	Directory	Account
PWRBKRTST2008	corp.ad.sentara.com	JJCOOPER_PBD
PWRBKRTST2012	corp.ad.sentara.com	JJCOOPER_PBD
PWRBKRTST2016	corp.ad.sentara.com	JJCOOPER_PBD
PWRBKRAUDITAP01	corp.ad.sentara.com	JJCOOPER_PBD

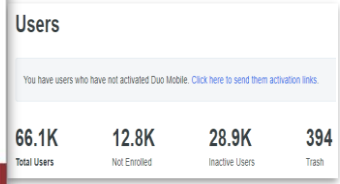
DUO 2Factor Authentication



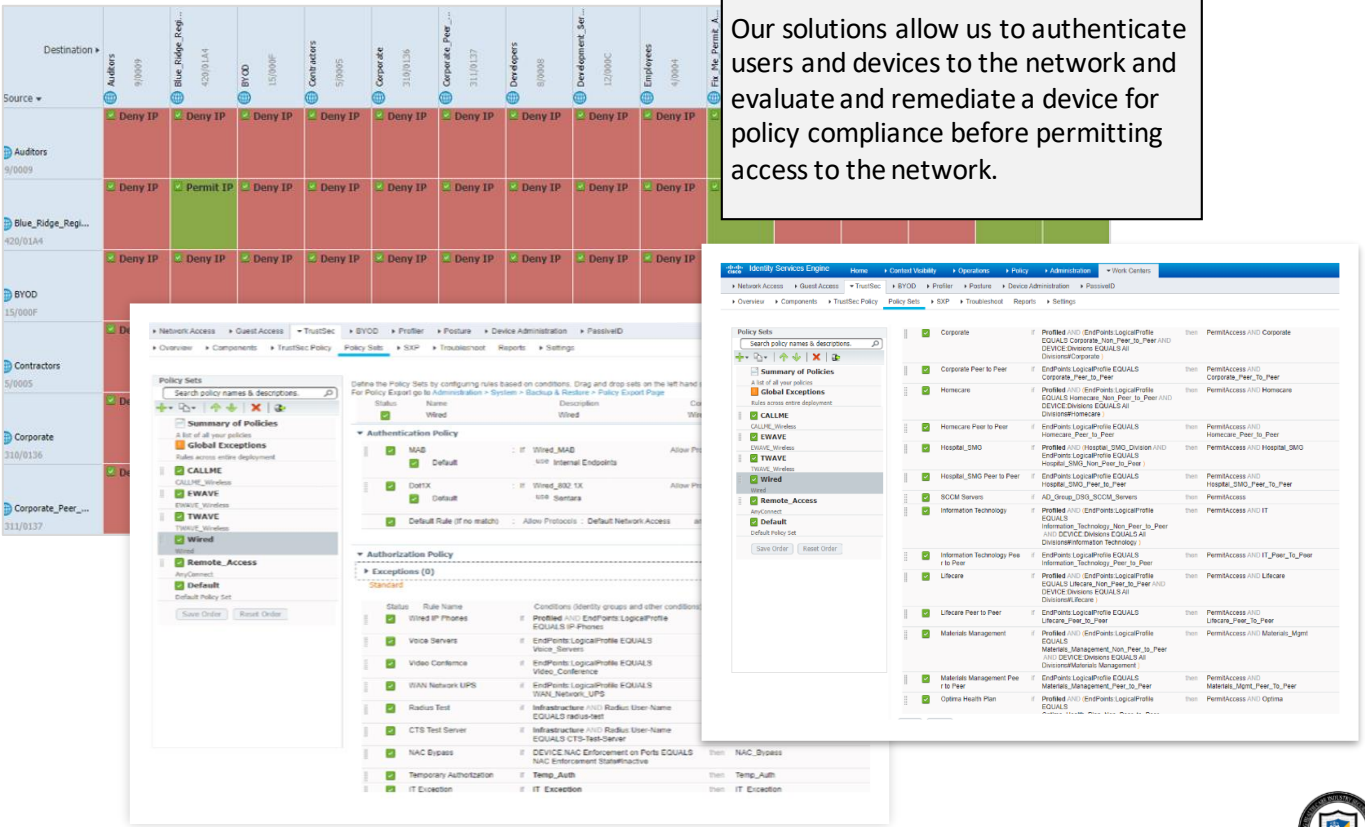


- 81.9% of breaches were the result of compromised credentials*
- 2 Step Logins secure Sentara and your personal information
- In order to meet increased Security standards, all workforce and business users who log in remotely (Outside of the Network), will be required to use DUO 2 Step Login.





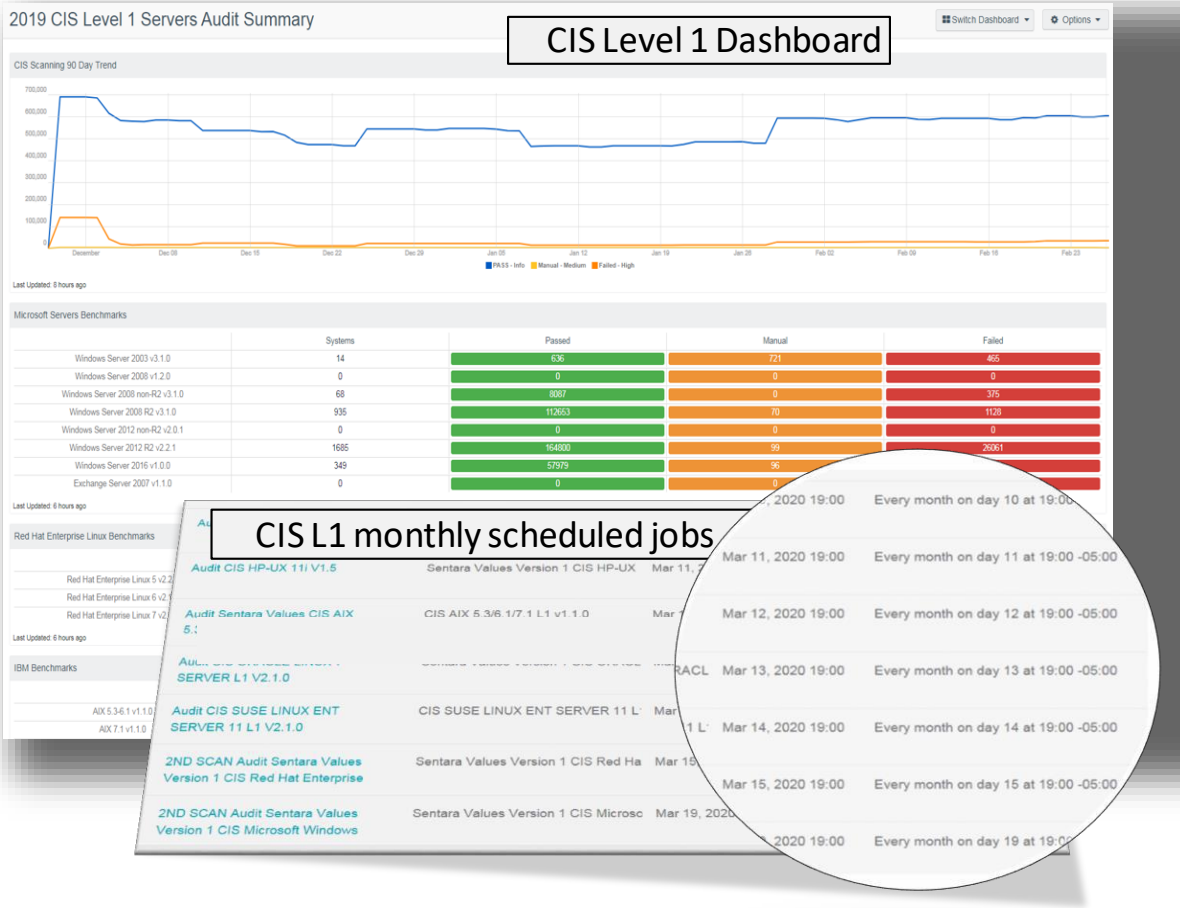
Network Access Control (NAC) ISE



Our solutions allow us to authenticate users and devices to the network and evaluate and remediate a device for policy compliance before permitting access to the network.

Vulnerability and Compliance Management

Configuration Management (CIS Level 1)



Patching and Virtual Patching

SENTARA

Standard: Security Patch Management Standard

Division: Sentara HealthCare

Original Date: 12-01-2012

Manual: Information Technology

Revision Date: 06-28-2017

Section: Information Security

Approved By: Chief Information Officer (CIO)

Location(s): CORPORATE, SCH, SLH, SMJH, SNGH, SNVMC, SOH, SPAH, SVBGH, SWRMC, SRMH, SAMC, SHRH, SLC, OPTIMA, SMG, SRMG, SE, PACE

Process Owner: Information Security GRC Office

Revision Date	Revision Description (Most Recent)
6/19/2013	Updated Policy to map directly to HITRUST governance requirements
11/10/2015	Reviewed; updated Location section
11/24/2017	Updated patching interval section and added Emergent vulnerability type-converted policy to a standard

Standard Statement:

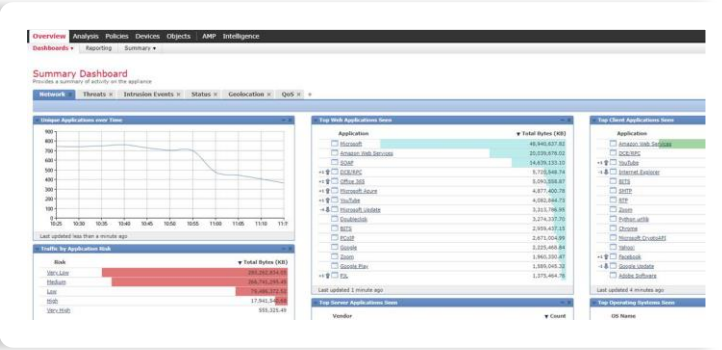
This standard applies to all workstations, laptops, and servers that are connected to the Sentara HealthCare network. A current and complete inventory of applications shall exist and be maintained to ensure effective technical vulnerability management.

Appropriate and timely action shall be taken in response to the identification of potential technical security vulnerabilities. Upon identification of potential security vulnerability, IT Security shall identify the associated risks and define the procedure that will be taken. Procedure shall include patching of vulnerable systems / applications and applying other compensating controls.

Security Patching Requirements:

Workstations

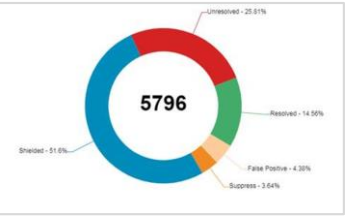
Desktops and laptops shall have automatic updates enabled or a central patching solution configured for



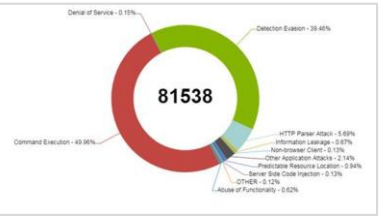
- Different patching intervals considered for internet facing assets.
- We utilize WAFs and IPSs when necessary to virtually patch fragile assets.

Vulnerability SLAs			
Internet Facing		**Internal**	
Emergent (OS)	3 Days	Emergent (OS)	7 Days
Emergent (Java)	7 Days	Emergent (Java)	30 Days
Emergent (3rd party)	7 Days	Emergent (3rd party)	30 Days
Critical / High (OS)	7 Days	Critical / High (OS)	30 Days
Critical / High (Java)	30 days	Critical / High (Java)	60 Days
Critical / High (3rd party)	30 days	Critical / High (3rd party)	60 Days

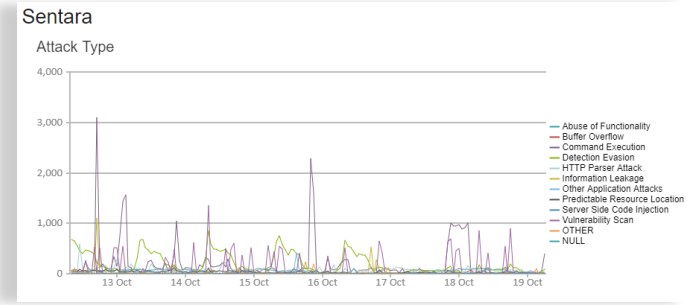
Total Vulnerabilities

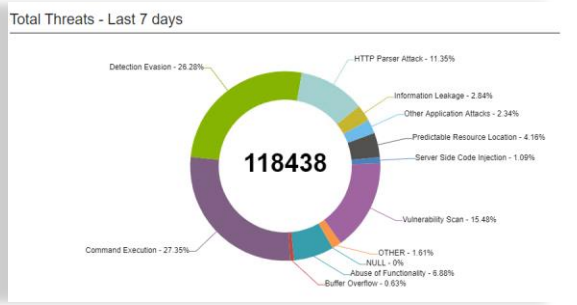


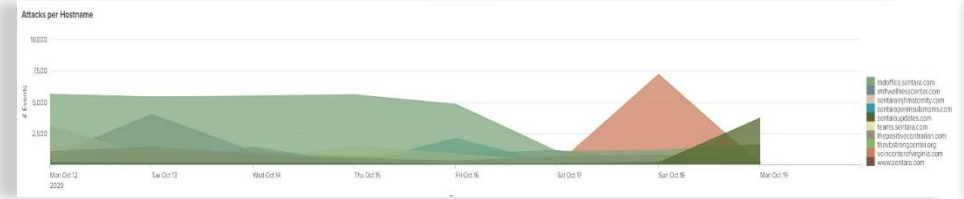
Total Threats – Last 7 days



WebApp Shielding (RedShield)

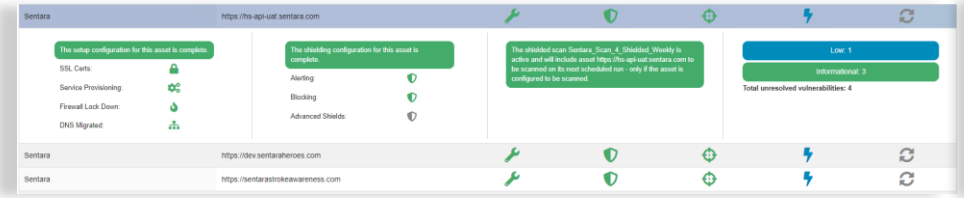


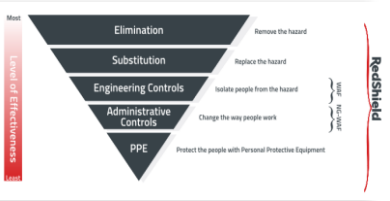




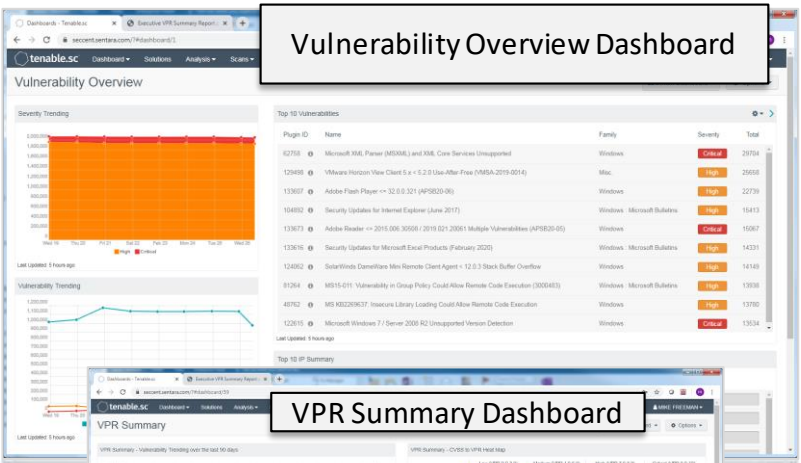
Attacks by Country - Last 7 days

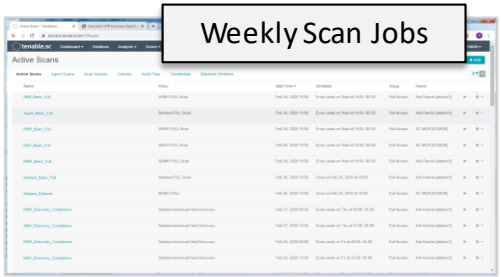
Country	Attack Count	Rate
United States	66284	55.4%
China	19848	16.6%
Canada	3742	3.1%
France	3041	2.5%
Russia	3036	2.5%
India	2485	2.1%
Germany	2382	2.0%
Netherlands	1691	1.4%

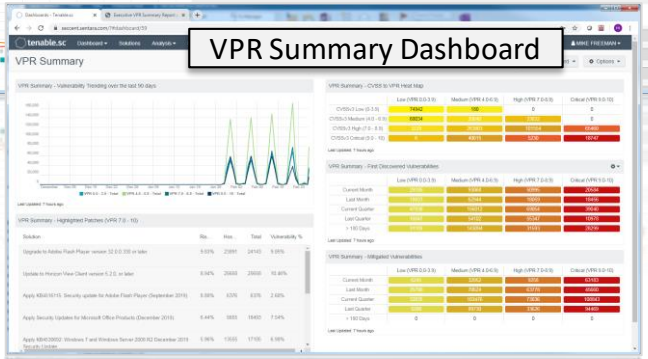


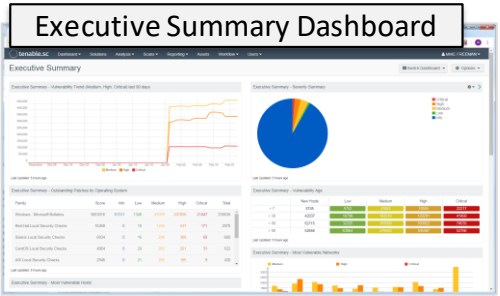


Weekly Vulnerability Scans (Tenable)

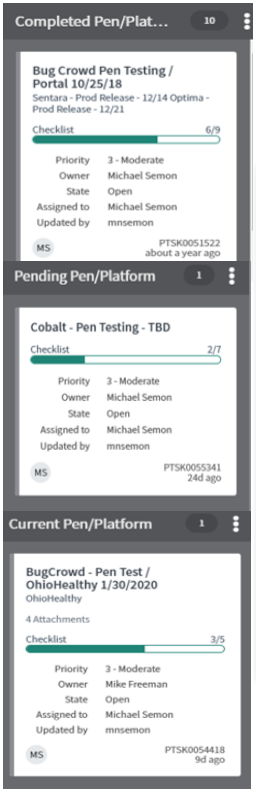




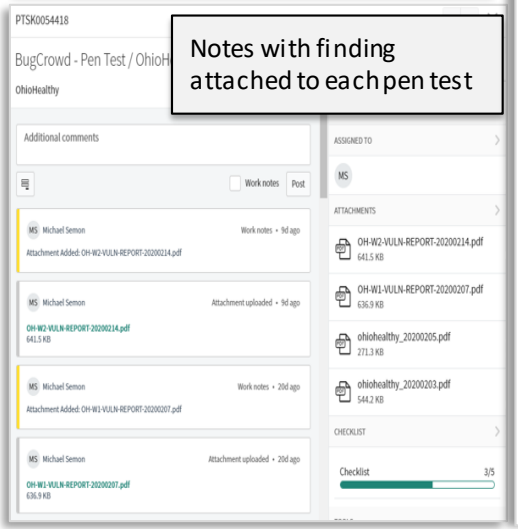




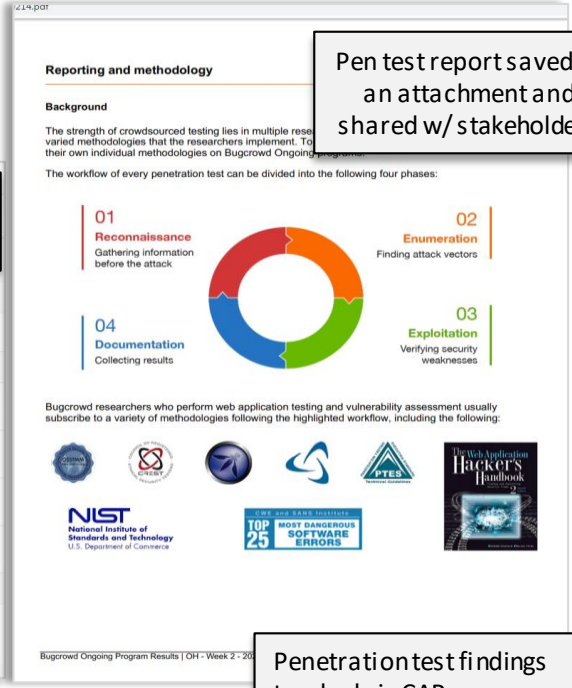
Penetration Testing



Pen testing performed several time a year by different vendors. Dashboard in ServiceNow showing pending, current and completed



Notes with finding attached to each pen test

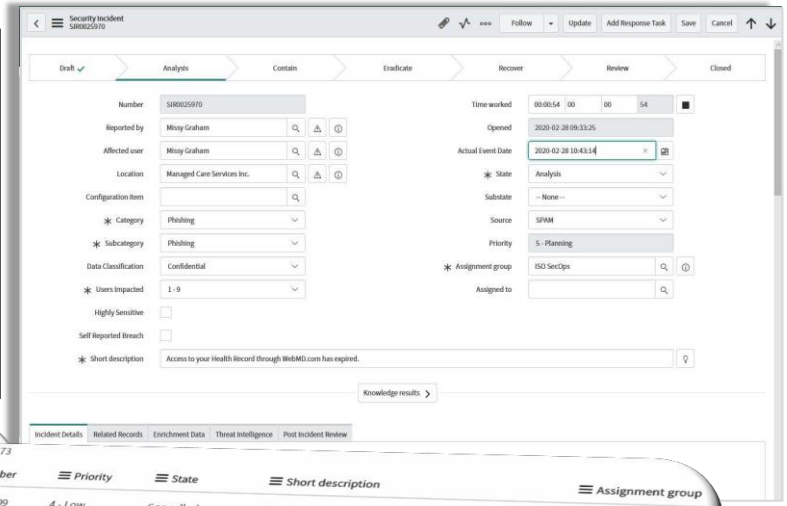


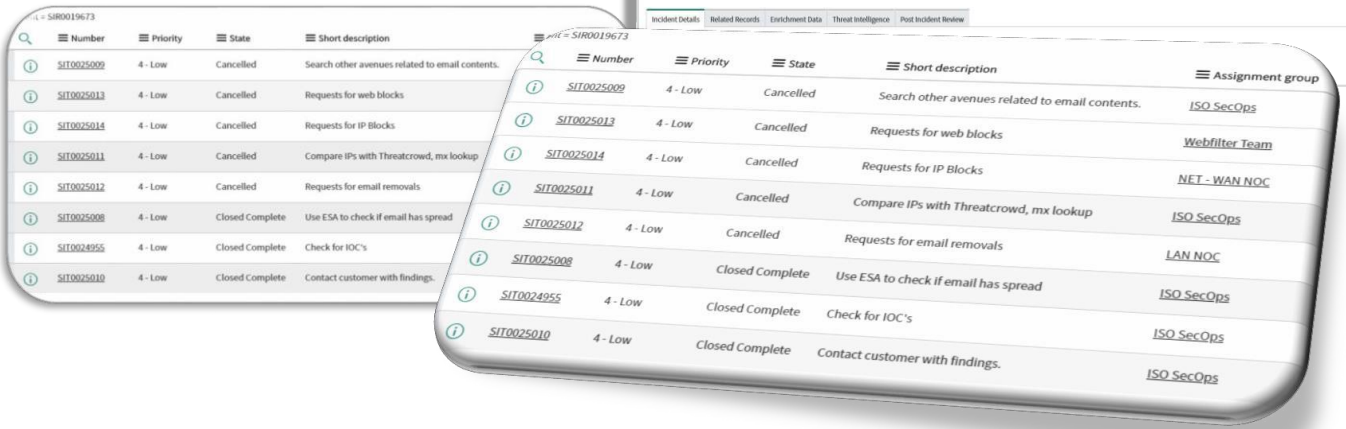
Pen test report saved as an attachment and shared w/ stakeholders

Penetration test findings tracked via CAPs

Malware Analysis and Response – SPAM Mailbox

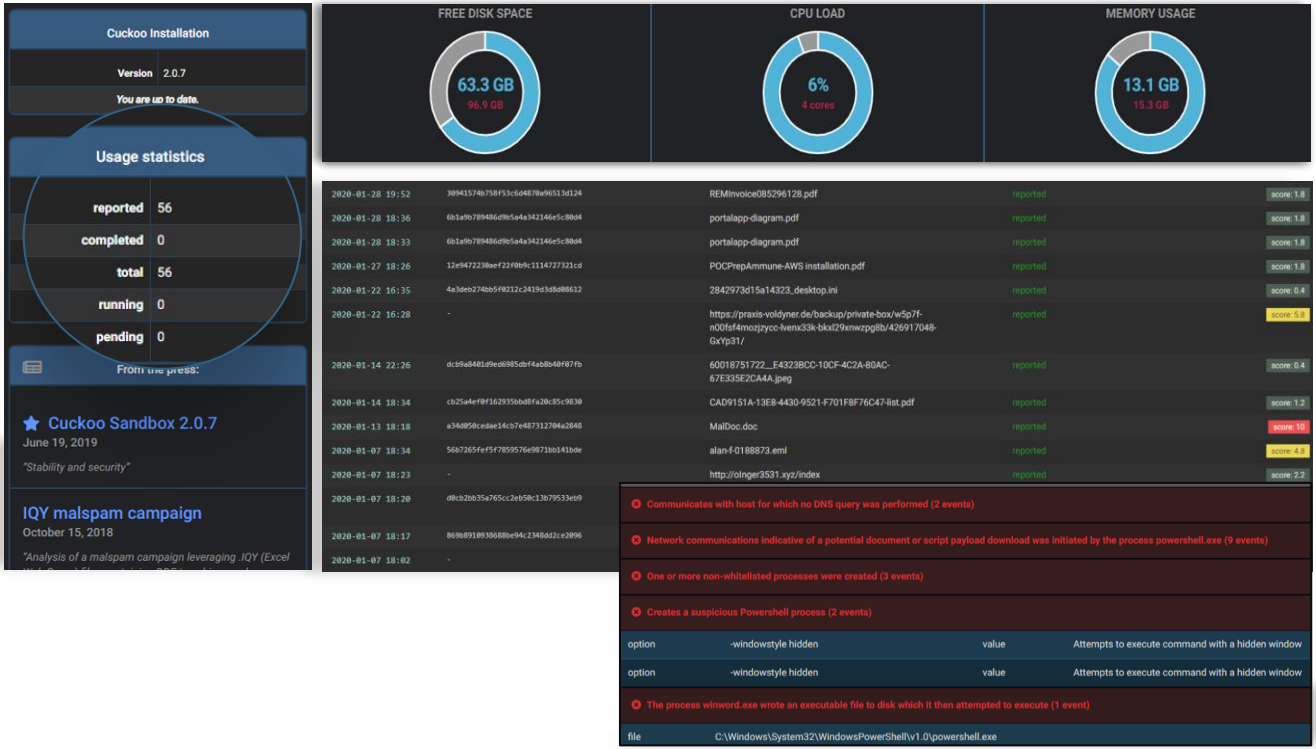
Suspected malicious e-mails are submitted to the Incident Response team for analysis. There are procedures as well as a secure workflow system in ServiceNow which is used to analyze submissions.





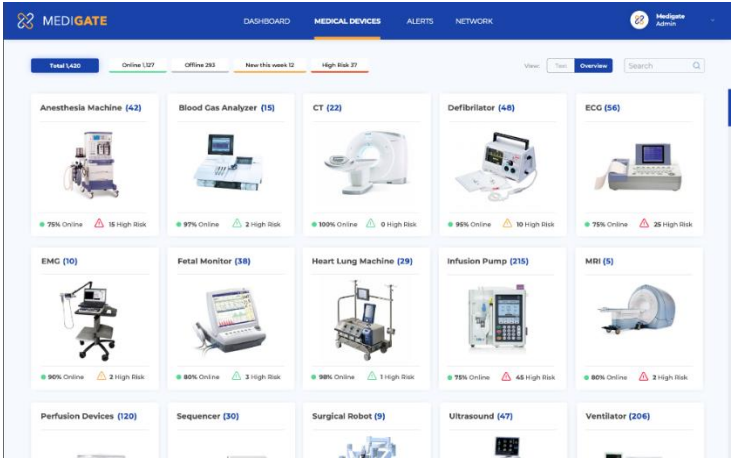
Number	Priority	State	Short description	Assignment group
SIT0025009	4 - Low	Cancelled	Search other avenues related to email contents.	ISO SecOps
SIT0025013	4 - Low	Cancelled	Requests for web blocks	Webfilter Team
SIT0025014	4 - Low	Cancelled	Requests for IP Blocks	NET - WAN NOC
SIT0025011	4 - Low	Cancelled	Compare IPs with Threatcrowd, mx lookup	ISO SecOps
SIT0025012	4 - Low	Cancelled	Requests for email removals	LAN NOC
SIT0025008	4 - Low	Closed Complete	Use ESA to check if email has spread	ISO SecOps
SIT0024955	4 - Low	Closed Complete	Check for IOC's	ISO SecOps
SIT0025010	4 - Low	Closed Complete	Contact customer with findings.	ISO SecOps

On Premise Malware Sandbox



Medical Device Security

- Mitigates patient safety risk
- Mitigates service line disruption due to ransomware
- Protects end-of-life operating systems, extending useful life of key clinical assets
- Fully integrated with Sentara Operations and Hospitals strategy for hospital asset management



MEDIGATE

Security Awareness and Training

Security Awareness and Training

Annual Regulatory One Link Learning

Annual Compliance Training
Annual Privacy Training
Annual Regulatory – IT Security
Annual Regulatory Challenge

Other Required Training

Information Technology Change Management

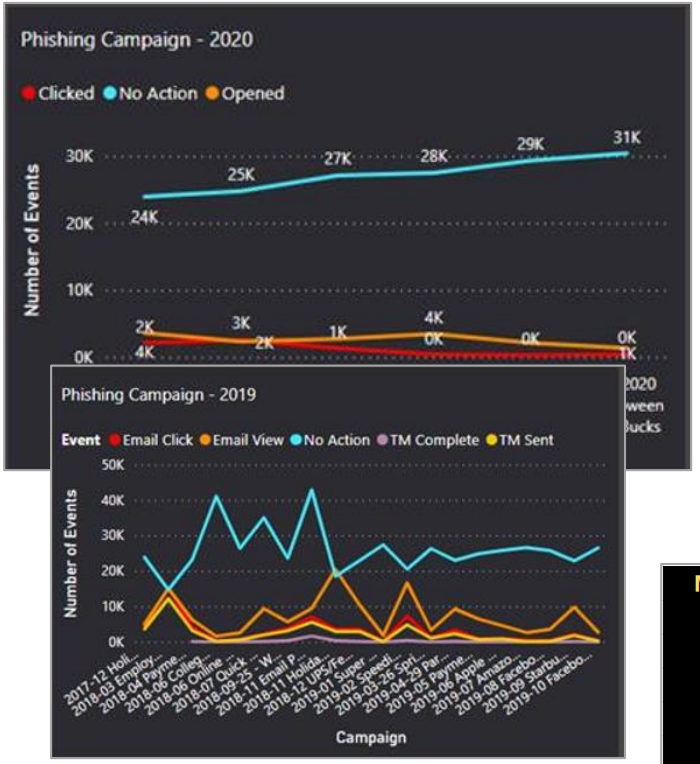
Cybersecurity Training Resources:

Cyber Security Awareness Month
Security Awareness Materials:

- Phishing 101
- Internet of Things – IOT Q/A
- Social Engineering
- Recognizing and Avoiding Business Email Compromise
- Mobile Device Security
- Protecting your Sensitive Information
- Using OpenDNS at Home
- Etc.

Monthly Phishing Campaigns

Phishing Campaign Dashboards



Phishing Campaign Teachable Moment

Month	Phished	Clicked
Jan	24039	2206
June	24854	2675
July	27197	1440
Aug	27590	475
Sept	29417	392
Oct	30506	497

Corporate Communications

US Hospitals and healthcare pr
and imminent cybercrime threa
Security department is engage
Human Services (HHS), the Cy
Agency (CISA), and the Federa
others and are actively monitor
intent. The primary entry point of thes
with links to websites outside of the Se

What You Can Do

Report Any Potential Incidents Im
Security incidents can happen anywhe
incident has occurred, make sure you
here to create an Incident record and

Stay Informed
Visit our cybersecurity resource page f
to reduce cybersecurity risks and prote
resources online.

Security Tips

Phishing:

- **Analyze the situation.** Beware
you to act quickly. For example "
"Click here now to receive $100
required".
- **Look but don't click.** Hover you
embedded in the body of the em

URGENT Security Awareness

- ***TIP:*** Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link that was shown in the example above reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address (see below) which signifies a phishing attempt.

- **Don't click on attachments.** Including malicious attachments that contain viruses and malware is a common phishing tactic. Don't open email attachments you weren't expecting.
- **Don't give up personal or financial information.** Legitimate banks and most other companies will never ask for personal credentials via email.

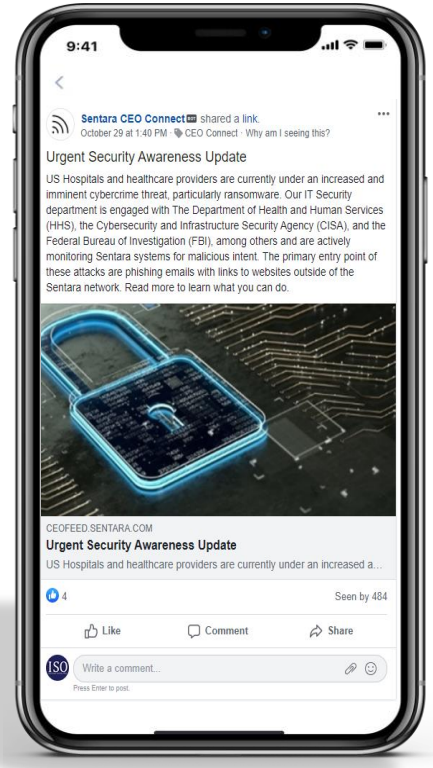
Phishing Tip Sheet

Continue Cybersafe Best Practices
Following remote work best practices, handling personal data safely, and watching out for digital scams like phishing. Please refer to our cybersecurity resource page for more information about these best practices.

Don't Hesitate to Ask If You Have Questions
If you have questions about the security or best practices, contact the Help Desk or email ISO_GRC@sentara.com and someone will be happy to speak with you.

Thank you for your support and commitment in staying cyber safe and helping all our team members, patients, members, and communities stay safe and secure online.

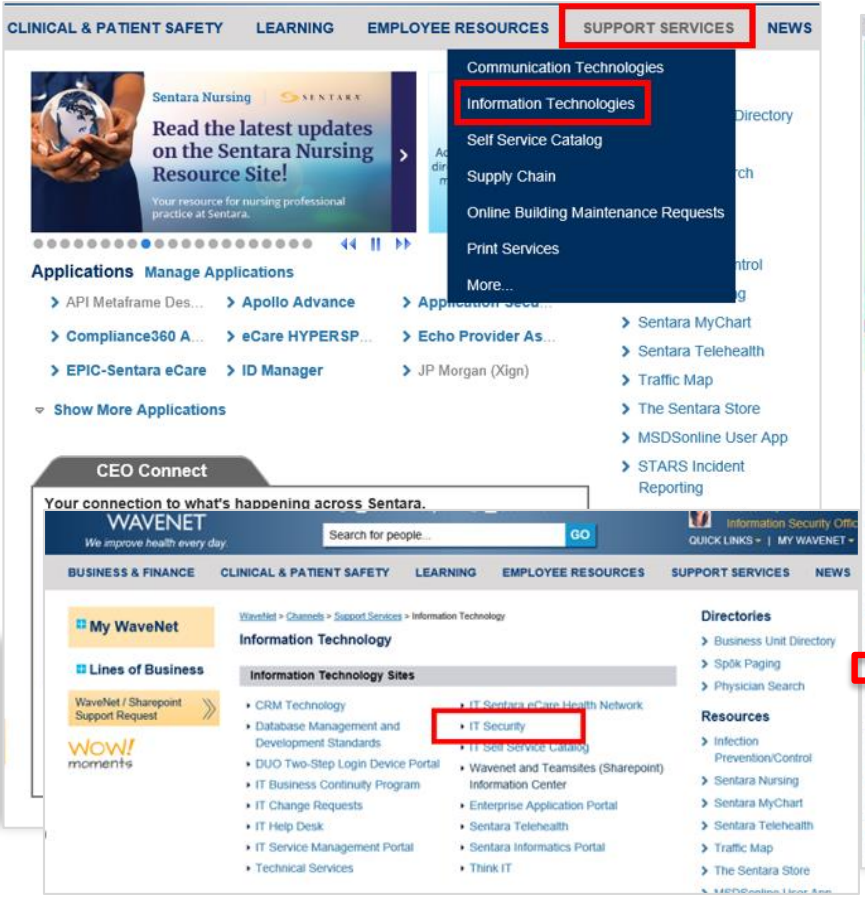
Dan Bowden
CISO, Information Security Office
Sentara Healthcare

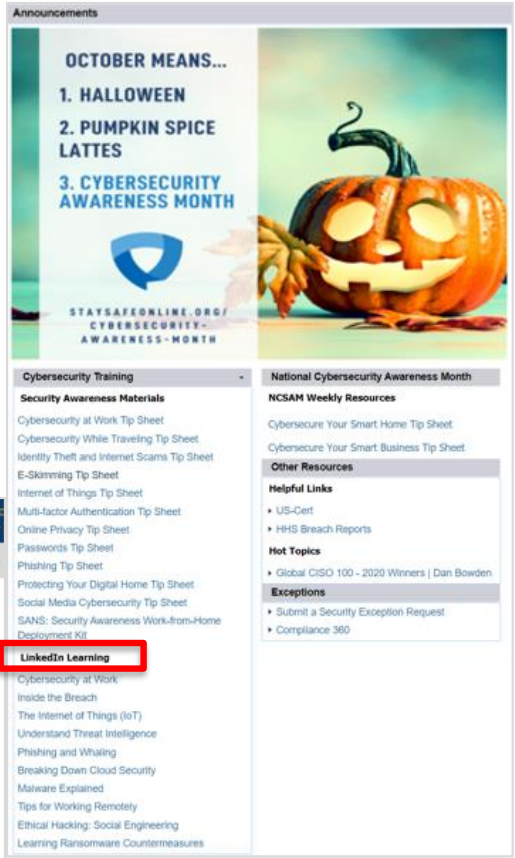


Education – Workplace by Facebook

Follow our ISO page throughout the month of October as we post weekly National Cyber Security updates! ISO will post important items throughout the year as we highlight resources and tips so YOU can play your part in keeping Sentara Cyber-Smart!

Cybersecurity Training Resource Wavenet Page





Recommendations

Blocking Consumer (Personal) Email

Block access to consumer mail such as Yahoo, Gmail, and AOL.

Some non-employees (physicians) may be inconvenienced, however, exceptions can be managed as necessary.

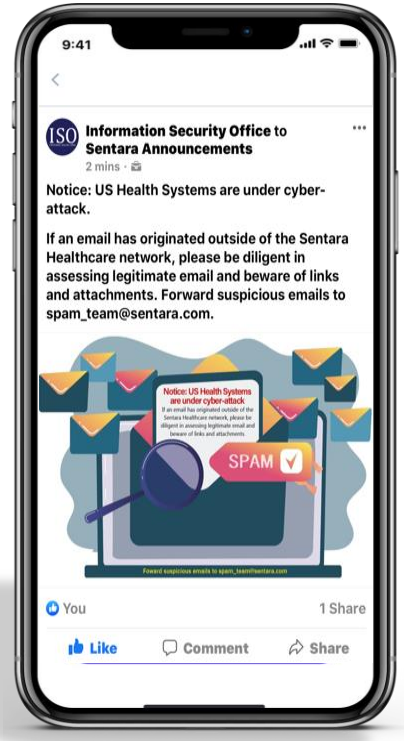
Increased Awareness Training

Workplace education
Weekly Communication(s)
Target Audience

Targeted education for phishing fails
Repeat clickers of phishing emails/campaigns

- Required Training
- Working with HR to utilize OneLink to share additional content with repeat clickers

Targeted emails w/required acknowledgment



Panel Discussion

Questions?

Do you follow us on Social Media?
Check us out at **@ask405d**

Linkedin.com/company/hhs-ask405d

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

The publication details the top five threats facing the healthcare industry and the ten practices to mitigate. Read the entire publication on our website: www.phe.gov/405d.