



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
<i>10 minutes</i>	Opening Remarks and Introductions	Julie Chua, HHS
<i>10 Minutes</i>	FDA Monitoring and Responding to Cyber Threats	Jessica Wilkerson
<i>10 Minutes</i>	Industry Response to Recent Threats	Dan Bowden
<i>20 Minutes</i>	Panel Discussion	All
<i>10 Minutes</i>	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 !

CSA Section 405
Improving Cybersecurity in the Healthcare Industry

Section 405(b):
Healthcare Industry
Preparedness Report

Section 405(c):
Healthcare Industry
Cybersecurity Task
Force

Section 405(d):
Aligning Healthcare
Industry Security
Approaches



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 remain safe and effective 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



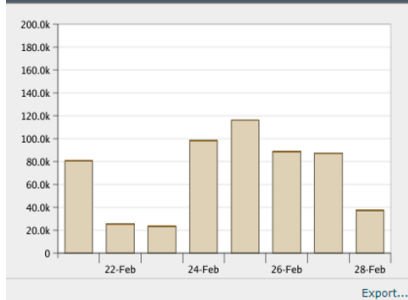
Cyber Threat Intel -- Ingest

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



Email Security Appliance

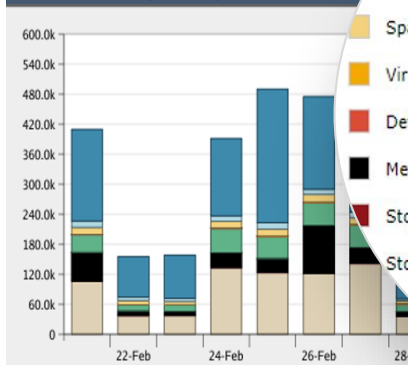
Overview > Outgoing Mail Graph



Overview > Outgoing Mail Summary

Message Processing	%	Messages
Spam Detected	0.0%	0
Virus Detected	0.0%	0
Detected by Advanced Malware Protection	0.0%	0
Messages with Malicious URLs	0.0%	0
Stopped by Content Filter	0.0%	0
Clean Messages	100.0%	557.2k
Total Messages Processed:		557.2k

Overview > Incoming Mail Graph



Overview > Incoming Mail Summary

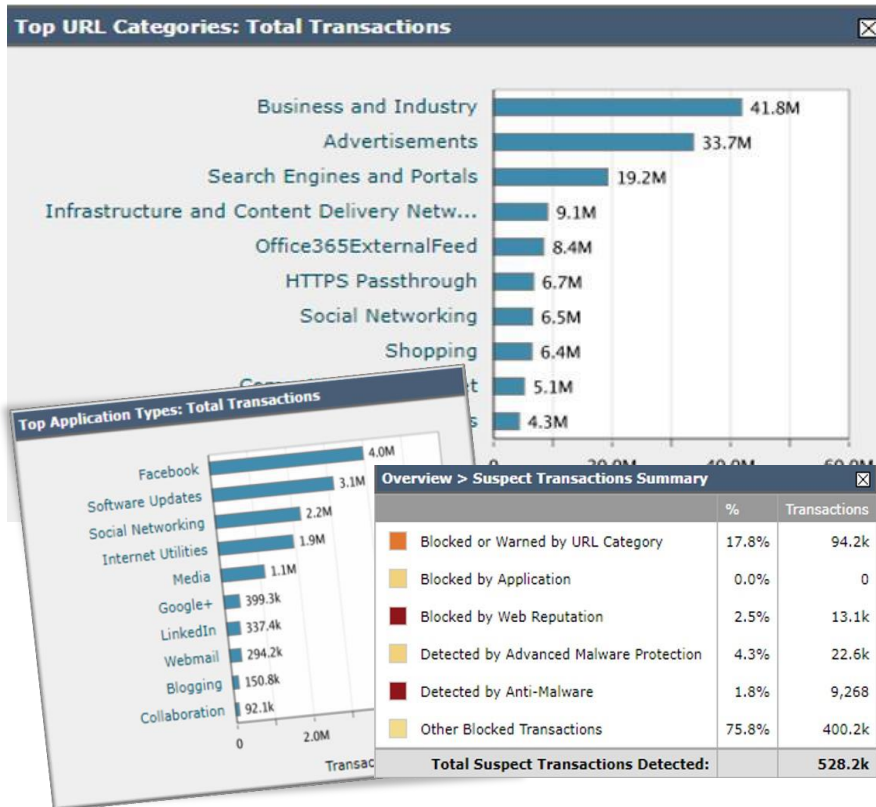
Message Delivery	%	Messages
Hard Bounced	0.0%	35.7k
Spam Detected	3.3%	91.5k
Virus Detected	0.0%	3
Detected by Advanced Malware Protection	0.0%	0
Messages with Malicious URLs	0.0%	190
Stopped by Content Filter	0.1%	3,210
Stopped by DMARC	0.0%	0
SPF Verification/Decryption Failed	0.0%	0
Stopped by Reputation Filtering	47.6%	125.0k
Stopped as Invalid Recipients	2.8%	7,500
Total Threat Messages		125.0k

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



Advanced Malware Protection for Endpoints



- Account protection
- Firewall & network protection
- App & browser control
- Device security
- Device performance & health
- Family options

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

Security at a glance

See what's happening with the security and health of your device and take any actions needed.



Virus & threat protection
No action needed.



Account protection
No action needed.



Firewall & network protection
No action needed.



App & browser control
Unknown



Device security
View status and manage hardware security features



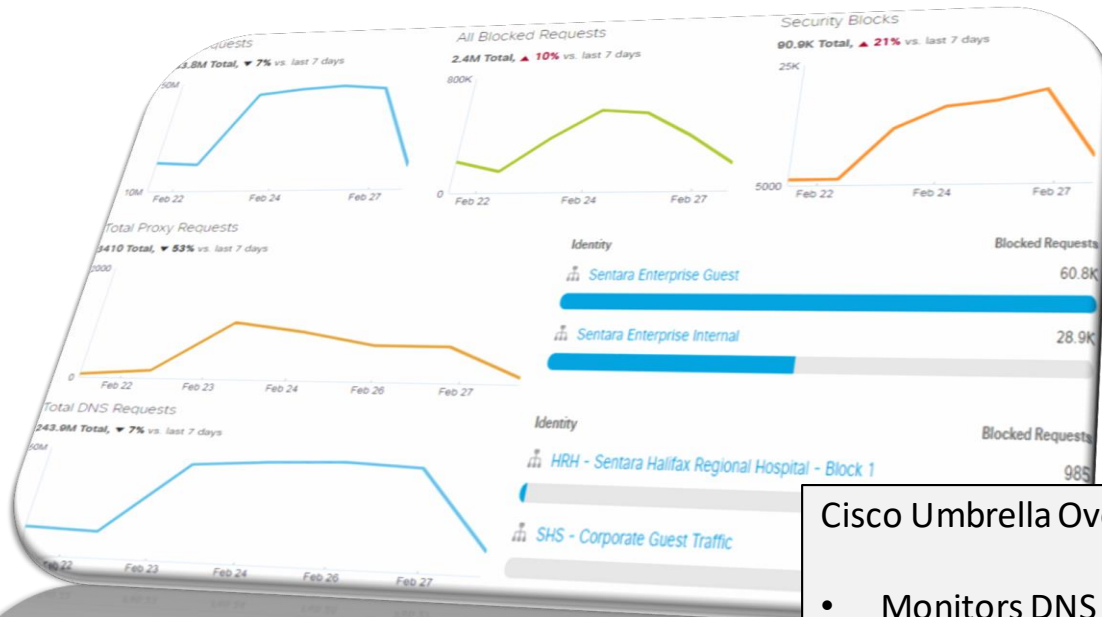
Device performance & health
No action needed.



Family options
Manage how your family uses their devices.



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

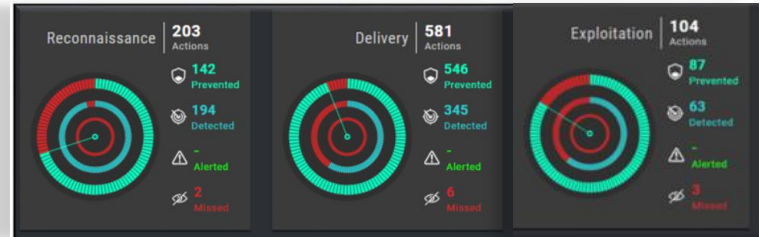
Optimization

- 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



PLEASE LOG IN

Duo two-factor login for jjcooper

Enter a passcode or select one of the following options:

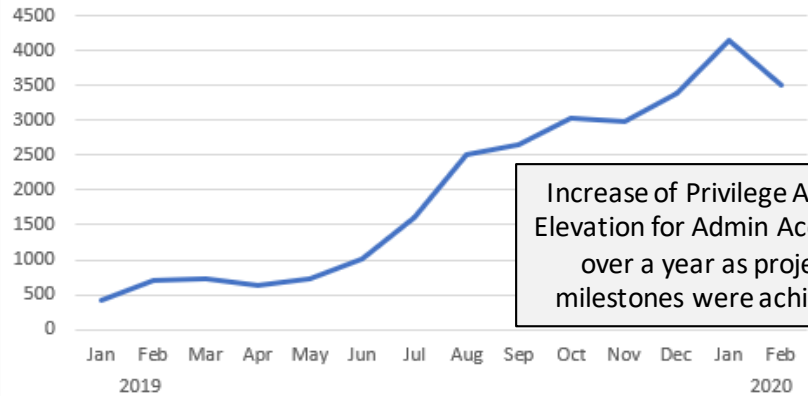
1. Duo Push to XXX-XXX-4735
2. Phone call to XXX-XXX-4735
3. SMS passcodes to XXX-XXX-4735 (next code starts with: 2)

Passcode or option (1-3):

Enter Response

SUBMIT CANCEL

Password Safe Usage



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

All Managed Accounts (776)

Page: 1 of 16

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

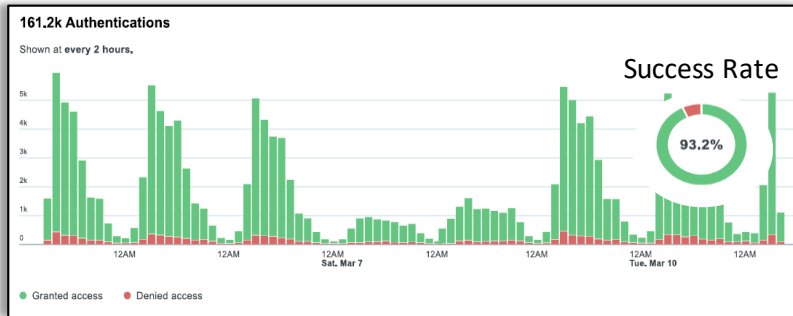
Managed Account Password Changed Daily and After Each Use

Servers and Privileged Accounts are Displayed

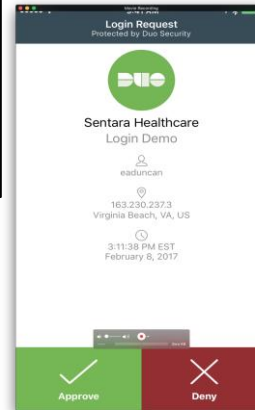
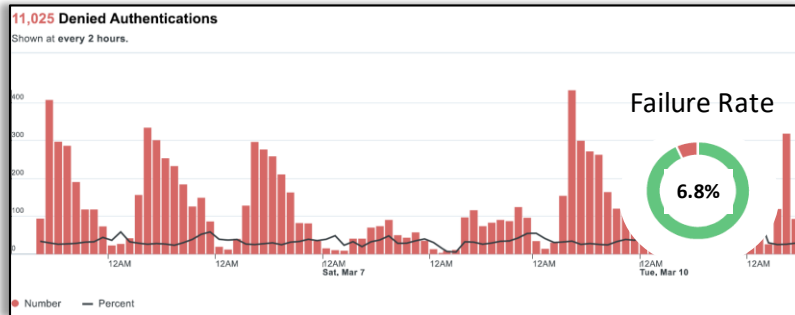
System	Directory	Account
PWRBKRTST2008	corp.ad.sentara.com	JJCOOPER_PBD
PWRBKRTST2012	corp.ad.sentara.com	JJCOOPER_PBD
PWRBKRTST2016	corp.ad.sentara.com	JJCOOPER_PBD
PWRBKRAUDITAP01	corp.ad.sentara.com	JJCOOPER_PBD



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.



Users

You have users who have not activated Duo Mobile. [Click here to send them activation links.](#)

66.1K Total Users	12.8K Not Enrolled	28.9K Inactive Users	394 Trash
-----------------------------	------------------------------	--------------------------------	---------------------



Network Access Control (NAC) ISE

Destination	Auditors	Blue_Ridge_Regi...	BYOD	Contractors	Corporate	Corporate_Peer...	Developers	Development_Ser...	Employees
Auditors	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Blue_Ridge_Regi...	Deny IP	Permit	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
BYOD	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Contractors	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Corporate	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Corporate_Peer...	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Developers	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Development_Ser...	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP
Employees	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP	Deny IP

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.

Network Access Control (NAC) ISE Configuration Screenshots:

- Policy Sets Configuration:** Shows a list of policy sets including Global Exceptions, CALLME, SWAVE, TWAVE, Wired, and Remote_Access. The Wired policy set is selected for configuration.
- Wired Policy Set Configuration:** Shows the configuration for the Wired policy set, including Authentication Policy (MAG, DORX) and Authorization Policy (Default, Exceptions).
- Exceptions List:** A table listing various exceptions such as Wired IP Phones, Voice Servers, Video Conferencing, and NAC Bypass.

Network Access Control (NAC) ISE Policy Sets List:

Policy Set	Configuration	Access
Corporate	EndPoints LogicalProfile EQUALS Corporate... AND DeviceDivisions EQUALS All	PermitAccess AND Corporate
Corporate Peer to Peer	EndPoints LogicalProfile EQUALS Corporate_Peer_To_Peer	PermitAccess AND Corporate_Peer_To_Peer
Homecare	EndPoints LogicalProfile EQUALS Homecare... AND DeviceDivisions EQUALS All	PermitAccess AND Homecare
Homecare Peer to Peer	EndPoints LogicalProfile EQUALS Homecare_Peer_To_Peer	PermitAccess AND Homecare_Peer_To_Peer
Hospital_SMO	EndPoints LogicalProfile EQUALS Hospital_SMO... AND DeviceDivisions EQUALS All	PermitAccess AND Hospital_SMO
Hospital_SMO Peer to Peer	EndPoints LogicalProfile EQUALS Hospital_SMO_Peer_To_Peer	PermitAccess AND Hospital_SMO_Peer_To_Peer
SCCM Servers	AD_Group_SMO_SCCM_Servers	PermitAccess AND SCCM_Servers
Information Technology	EndPoints LogicalProfile EQUALS Information_Technology... AND DeviceDivisions EQUALS All	PermitAccess AND IT
Information Technology Peer to Peer	EndPoints LogicalProfile EQUALS Information_Technology_Peer_To_Peer	PermitAccess AND IT_Peer_To_Peer
Litcoac	EndPoints LogicalProfile EQUALS Litcoac... AND DeviceDivisions EQUALS All	PermitAccess AND Litcoac
Litcoac Peer to Peer	EndPoints LogicalProfile EQUALS Litcoac_Peer_To_Peer	PermitAccess AND Litcoac_Peer_To_Peer
Materials Management	EndPoints LogicalProfile EQUALS Materials_Management... AND DeviceDivisions EQUALS All	PermitAccess AND Materials_Mgmt
Materials Management Peer to Peer	EndPoints LogicalProfile EQUALS Materials_Management_Peer_To_Peer	PermitAccess AND Materials_Mgmt_Peer_To_Peer
Optima Health Plan	EndPoints LogicalProfile EQUALS Optima_Health_Plan... AND DeviceDivisions EQUALS All	PermitAccess AND Optima

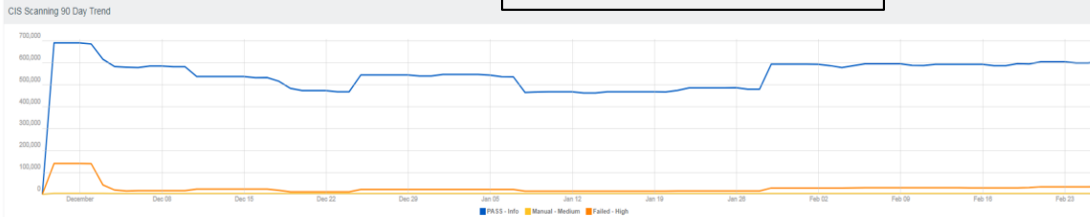


Vulnerability and Compliance Management Configuration Management (CIS Level 1)

2019 CIS Level 1 Servers Audit Summary

CIS Level 1 Dashboard

Switch Dashboard Options



Last Updated: 6 hours ago

Microsoft Servers Benchmarks

Benchmark	Systems	Passed	Manual	Failed
Windows Server 2003 v3.1.0	14	636	721	465
Windows Server 2008 v1.2.0	0	0	0	0
Windows Server 2008 non-R2 v3.1.0	68	8887	0	375
Windows Server 2008 R2 v3.1.0	935	112653	70	1128
Windows Server 2012 non-R2 v2.0.1	0	0	0	0
Windows Server 2012 R2 v2.2.1	1685	154800	59	2091
Windows Server 2016 v1.0.0	349	57979	96	0
Exchange Server 2007 v1.1.0	0	0	0	0

Last Updated: 6 hours ago

Red Hat Enterprise Linux Benchmarks

Benchmark	Systems	Passed	Manual	Failed	Scheduled Job
Audit CIS HP-UX 11i V1.5	Sentara Values Version 1 CIS HP-UX	Mar 11, 2020	Mar 11, 2020 19:00	Every month on day 10 at 19:00	2020 19:00
Audit Sentara Values CIS AIX 5.1	CIS AIX 5.3/6.1/7.1 L1 v1.1.0	Mar 11, 2020	Mar 12, 2020 19:00	Every month on day 12 at 19:00 -05:00	2020 19:00
Audit CIS SUSE LINUX ENT SERVER L1 V2.1.0	CIS SUSE LINUX ENT SERVER 11 L1 V2.1.0	Mar 11, 2020	Mar 13, 2020 19:00	Every month on day 13 at 19:00 -05:00	2020 19:00
2ND SCAN Audit Sentara Values Version 1 CIS Red Hat Enterprise	Sentara Values Version 1 CIS Red Hat Enterprise	Mar 15, 2020	Mar 14, 2020 19:00	Every month on day 14 at 19:00 -05:00	2020 19:00
2ND SCAN Audit Sentara Values Version 1 CIS Microsoft Windows	Sentara Values Version 1 CIS Microsoft Windows	Mar 19, 2020	Mar 15, 2020 19:00	Every month on day 15 at 19:00 -05:00	2020 19:00
					2020 19:00
					Every month on day 19 at 19:00



Patching and Virtual Patching



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, SINGH, 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 HTRUST 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.

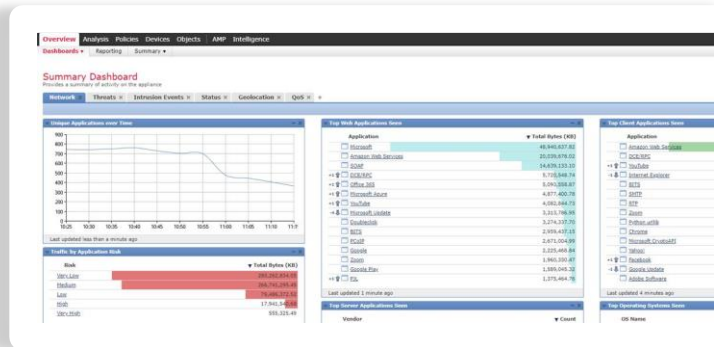
Appropriate and timely action shall be taken in response to the identification of potential technical security vulnerabilities. Upon identification of potential security vulnerability, IT Security shall identify the associated risks and define the procedure that will be taken. Procedure shall include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

Security Patching Requirements:

Workstations

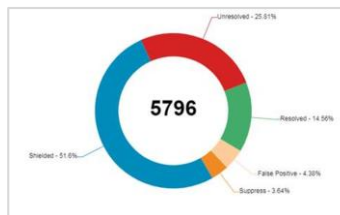
Desktops and laptops shall have automatic updates enabled or a central patching solution configured for

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

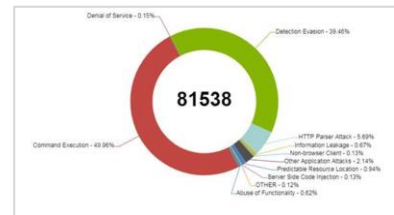


- Different patching intervals considered for internet facing assets.
- We utilize WAFs and IPSs when necessary to virtually patch fragile assets.

Total Vulnerabilities



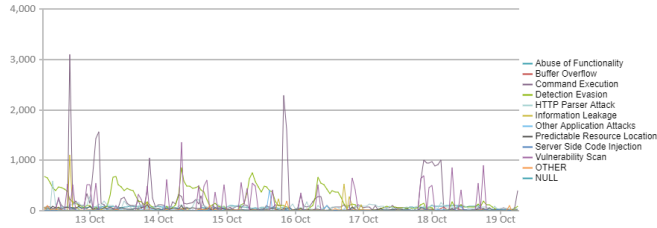
Total Threats – Last 7 days



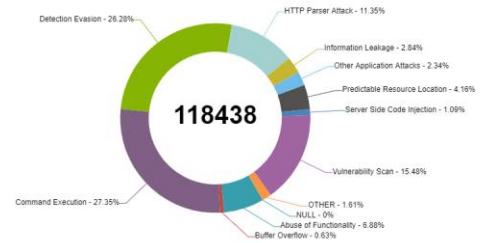
WebApp Shielding (RedShield)

Sentara

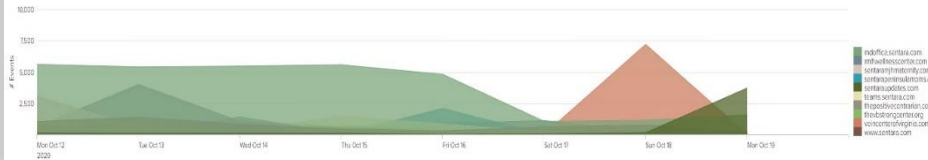
Attack Type



Total Threats - Last 7 days



Attacks per Hostname



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	2483	2.1%
Germany	2382	2.0%
Netherlands	1951	1.4%

Asset: <https://hs-api-us1.sentara.com>

Configuration Status:

- SSL Certs: The setup configuration for this asset is complete.
- Service Provisioning: Complete.
- Firewall Lock Down: Complete.
- DNS Migrated: Complete.
- Alerting: On.
- Blocking: On.
- Advanced Shields: On.

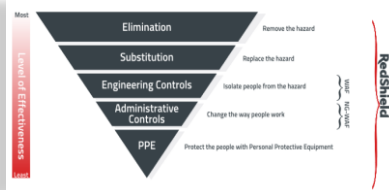
Scan Status: The scheduled scan for this asset is active and will include asset <https://hs-api-us1.sentara.com> to be scanned on its next scheduled run only if the asset is configured to be scanned.

Level: 1 (Informational)

Total unresolved vulnerabilities: 4

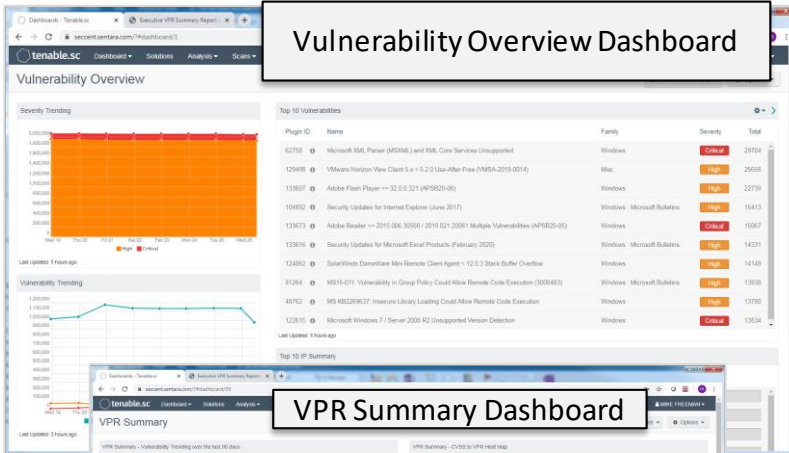
Summary of assets:

Asset URL	Configuration	Alerting	Blocking	Advanced Shields	Scan Status	Level	Unresolved Vulnerabilities
https://dev.sentaraheroes.com	Complete	On	On	On	Active	1	0
https://sentarastrokeawareness.com	Complete	On	On	On	Active	1	0



Weekly Vulnerability Scans (Tenable)

Vulnerability Overview Dashboard



Weekly Scan Jobs

Name	Start Time	Status
Active_Scan_1	Feb 20, 2020 10:00	Failed
Active_Scan_2	Feb 20, 2020 10:00	Failed
Active_Scan_3	Feb 20, 2020 10:00	Failed
Active_Scan_4	Feb 20, 2020 10:00	Failed
Active_Scan_5	Feb 20, 2020 10:00	Failed
Active_Scan_6	Feb 20, 2020 10:00	Failed
Active_Scan_7	Feb 20, 2020 10:00	Failed
Active_Scan_8	Feb 20, 2020 10:00	Failed
Active_Scan_9	Feb 20, 2020 10:00	Failed
Active_Scan_10	Feb 20, 2020 10:00	Failed

Executive Summary Dashboard



VPR Summary Dashboard



Penetration Testing

Completed Pen/Platform 10

Bug Crowd Pen Testing / Portal 10/25/18
Sentara - Prod Release - 12/14 Optima - Prod Release - 12/21

Checklist 6/9

Priority 3 - Moderate
Owner Michael Semon
State Open
Assigned to Michael Semon
Updated by mnsemon

PTSK0051522
about a year ago

Pending Pen/Platform 1

Cobalt - Pen Testing - TBD

Checklist 2/7

Priority 3 - Moderate
Owner Michael Semon
State Open
Assigned to Michael Semon
Updated by mnsemon

PTSK0055341
24d ago

Current Pen/Platform 1

BugCrowd - Pen Test / OhioHealthy 1/30/2020
OhioHealthy

4 Attachments

Checklist 3/5

Priority 3 - Moderate
Owner Mike Freeman
State Open
Assigned to Michael Semon
Updated by mnsemon

PTSK0054418
9d ago

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

PTSK0054418

BugCrowd - Pen Test / OhioHealthy

OhioHealthy

Additional comments

Work notes Post

ASSIGNED TO MS

ATTACHMENTS

- MS Michael Semon Work notes • 5d ago
Attachment Added: OH-WI-VULN-REPORT-20200214.pdf 641.5 KB
- MS Michael Semon Attachment uploaded • 5d ago
OH-WI-VULN-REPORT-20200214.pdf 641.5 KB
- MS Michael Semon Work notes • 20d ago
Attachment Added: OH-WI-VULN-REPORT-20200207.pdf 636.9 KB
- MS Michael Semon Attachment uploaded • 20d ago
ohiohealthy_20200205.pdf 271.3 KB
- MS Michael Semon Attachment uploaded • 20d ago
ohiohealthy_20200203.pdf 544.2 KB

CHECKLIST

Checklist 3/5

Reporting and methodology

Background

The strength of crowdsourced testing lies in multiple research methodologies that the researchers implement. To their own individual methodologies on Bugcrowd Ongoing Program.

The workflow of every penetration test can be divided into the following four phases:

01

Reconnaissance

Gathering information before the attack

02

Enumeration

Finding attack vectors

03

Exploitation

Verifying security weaknesses

04

Documentation

Collecting results

Bugcrowd researchers who perform web application testing and vulnerability assessment usually subscribe to a variety of methodologies following the highlighted workflow, including the following:

TOP 25 MOST DANGEROUS SOFTWARE ERRORS

Bugcrowd Ongoing Program Results | OH - Week 2 - 2020

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.

The screenshot shows a ServiceNow Security Incident record for SIR0025010. The record is in the 'Analysis' stage. Key details include:

- Number:** SIR0025010
- Reported by:** Missy Graham
- Affected user:** Missy Graham
- Location:** Managed Care Services Inc.
- Configuration item:** (Empty)
- Category:** Phishing
- Subcategory:** Phishing
- Data Classification:** Confidential
- Users Impacted:** 1 - 9
- Highly Sensitive:** (Unchecked)
- Self Reported Breach:** (Unchecked)
- Short description:** Access to your Health Record through WebMD.com has expired.
- Time worked:** 00:00:54
- Opened:** 2020-02-28 09:33:25
- Actual Event Date:** 2020-02-28 10:43:14
- State:** Analysis
- Substate:** None
- Source:** SPAM
- Priority:** 5 - Planning
- Assignment group:** ISO SecOps

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

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

Cuckoo Installation

Version 2.0.7

You are up to date.

Usage statistics

reported	56
completed	0
total	56
running	0
pending	0

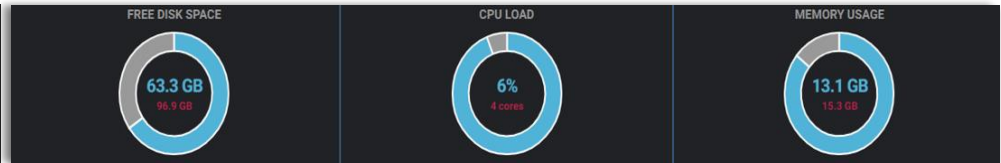
From `user@pre88`:

Cuckoo Sandbox 2.0.7
June 19, 2019

"Stability and security"

IQY malspam campaign
October 15, 2018

"Analysis of a malspam campaign leveraging IQY (Excel ..."



Time	File Name	Status	Score
2020-01-28 19:52	38941574b78f153c64878e95513d124	reported	score: 1.8
2020-01-28 18:36	661a7b789486d965a4342146e5c8804	reported	score: 1.8
2020-01-28 18:33	661a7b789486d965a4342146e5c8804	reported	score: 1.8
2020-01-27 18:26	12e9472238ae72f8b9c1114727321cd	reported	score: 1.8
2020-01-22 16:35	4a36e274b25f9212c241363d8986612	reported	score: 0.4
2020-01-22 16:28	-	https://praxis-voldyner.de/backup/private-box/w5p7f-n00fst4mozjzyc-lvenc33k-bkx29mwzpg8b/426917048-Gx1p31/	Score: 0.8
2020-01-14 22:26	dc99a8481d9cd985dbf4e6b848f97fb	reported	score: 0.4
2020-01-14 18:34	cb254ef8f7162915b5b8f428c85c938	CAD9151A-13E8-4430-9521-F701F876C47-list.pdf	score: 1.2
2020-01-13 18:18	a34895c8daa14c37e487312794a2848	MalDoc.doc	score: 10
2020-01-07 18:34	56d725fef72f7899576e9871b15141de	alan.f0188873.eml	score: 4.1
2020-01-07 18:23	-	http://olnger3531.xyz/index	score: 2.2

- 🔴 Communicates with host for which no DNS query was performed (2 events)
- 🔴 Network communications indicative of a potential document or script payload download was initiated by the process powershell.exe (9 events)
- 🔴 One or more non-whitelisted processes were created (3 events)
- 🔴 Creates a suspicious Powershell process (2 events)

option	-windowstyle hidden	value	Attempts to execute command with a hidden window
option	-windowstyle hidden	value	Attempts to execute command with a hidden window

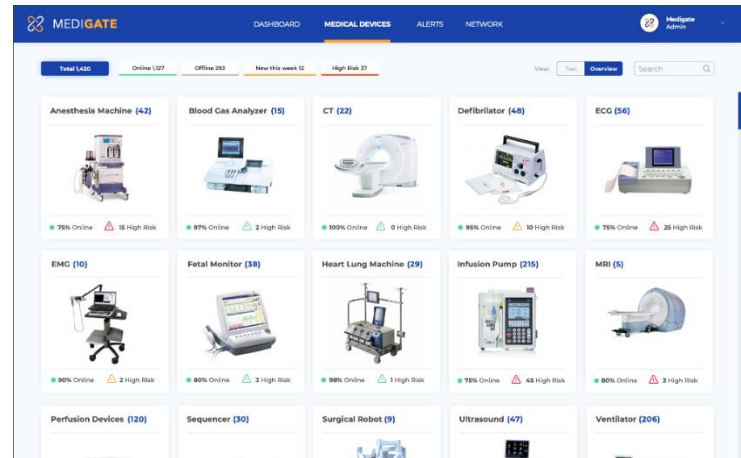
- 🔴 The process winword.exe wrote an executable file to disk which it then attempted to execute (1 event)

file	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
------	---



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.

LinkedIn Learning



5 of the Most In-Demand Hard Skills for 2020

HAVEN'T LOGGED INTO YOUR LINKEDIN LEARNING ACCOUNT YET?

When clicking on the links below, just sign in with the single sign on button.

While the most in-demand soft skills are the same, the most in-demand hard skills are the ones that are in high demand.

As companies continue to collect and analyze data, they can help interpret and take action on it.

Here are 5 from LinkedIn Learning:

- Blockchain was born in 2009 to support digital transactions, store, validate, authorize, and manage data.

BE ON THE LOOKOUT!!
New Training & Education
COMING SOON!

LEAVE YOUR SEAT? CTRL ALT DEL

DON'T GET HOOKED!! STAY ALERT FOR PHISHING EMAILS

How to protect yourself...

1. Identify suspicious links and avoid clicking on them.
2. Don't click on links in unsolicited emails or text messages.
3. Don't click on links in social media posts or messages.

INFORMATION SECURITY SENTARA

onelink
LEARNING

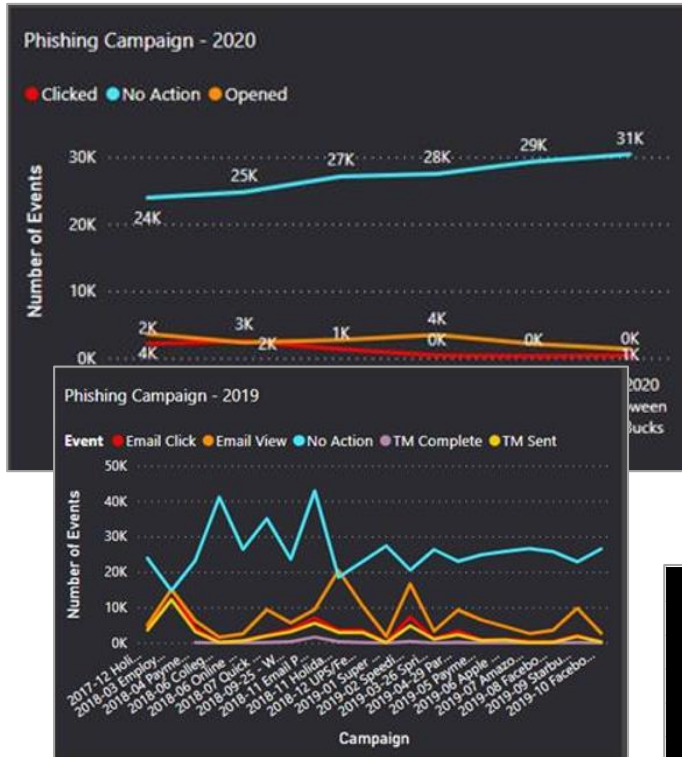
INFORMATION SECURITY SENTARA

What is OneLink Learning?
It is Sentara's Learning Management System which uses the Oracle PeopleSoft ELM 9.2 technology. Although it is a separate application, it is fully integrated with OneLink, Sentara's Integrated Human Resources & Payroll solution.



Monthly Phishing Campaigns

Phishing Campaign Dashboards



Phishing Campaign Teachable Moment

INFORMATION SECURITY

SENTARA

Oops! The email you just responded to was a fake phishing email. Don't worry! It was sent to you to help you learn how to avoid real attacks. Please do not share your experience with colleagues, so they can learn too.

Stay Alert for Phishing Emails

Dangerous links and downloading infected files puts you and your employer at risk

Beware of These Warning Signs

- Unsolicited emails that urge you to act quickly
- Deals and offers that seem too good to be true
- Unsolicited emails that contrain attachments
- Random requests to download forms, fill them out, and return them

Email Safety Tips

- Hover over a link to see its true source; links that look legitimate can be masks for dangerous links
- Do not click or respond to suspicious emails
- Do not download any attachments in suspicious emails
- Forward suspicious emails to Spam_Team@sentara.com
- Ask your IT department for advice if you're unsure

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 providers are currently under an increased and imminent cybercrime threat, particularly ransomware. Our IT Security department is engaged with The Department of Health and Human Services (HHS), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI), among others and are actively monitoring Sentara systems for malicious intent. The primary entry point of these attacks are phishing emails with links to websites outside of the Sentara network. Read more to learn what you can do.

What You Can Do

Report Any Potential Incidents Immediately
If a security incident can happen anywhere, make sure you report it [here](#) to create an Incident record and receive assistance.

Stay Informed

Visit our [cybersecurity resource page](#) for the latest news and resources to reduce cybersecurity risks and protect your data. All resources are online.

Security Tips

Phishing:

- **Analyze the situation.** Beware of offers that seem too good to be true. You may be asked to act quickly. For example, "Click here now to receive \$100,000. No questions asked." "Click here now to receive \$100,000. No questions asked." "Click here now to receive \$100,000. No questions asked."
- **Look but don't click.** Hover your mouse over links embedded in the body of the email to see the real web address, as shown in the example below with the yellow background. The string of cryptic numbers looks nothing like the company's web address (see below) which signifies a phishing attempt.

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 message 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

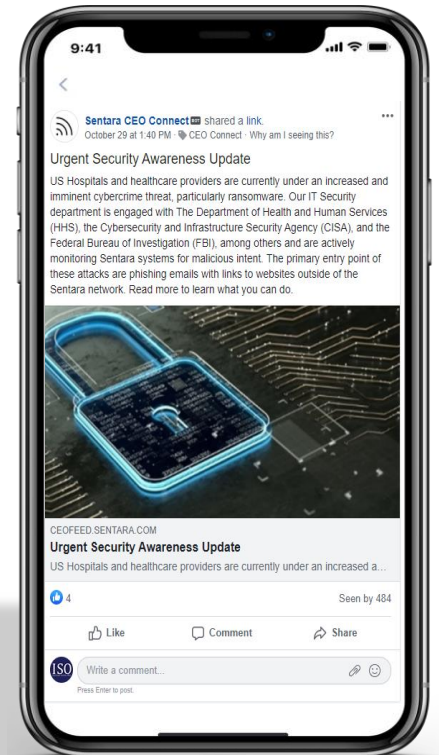
Following remote work best practices, handling personal data safely, and watching out for digital scams like phishing. Please refer to our cybersecurity resource page for more information about these best practices.

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

CLINICAL & PATIENT SAFETY LEARNING EMPLOYEE RESOURCES **SUPPORT SERVICES** NEWS

Read the latest updates on the Sentara Nursing Resource Site!

Applications Manage Applications

- API Metaframe Des...
- Apollo Advance
- Compliance360 A...
- eCare HYPERSP...
- EPIC-Sentara eCare
- ID Manager
- JP Morgan (Xign)
- Sentara MyChart
- Sentara Telehealth
- Traffic Map
- The Sentara Store
- MSDSOnline User App
- STARS Incident Reporting

CEO Connect

Your connection to what's happening across Sentara.

WAVENET
We improve health every day.

Search for people... **GO**

Information Security Office
QUICK LINKS - | MY WAVENET -

BUSINESS & FINANCE CLINICAL & PATIENT SAFETY LEARNING EMPLOYEE RESOURCES **SUPPORT SERVICES** NEWS

My WaveNet

Wavenet > Channels > Support Services > Information Technology

Information Technology

Information Technology Sites

- CRM Technology
- Database Management and Development Standards
- DUO Two-Step Login Device Portal
- IT Business Continuity Program
- IT Change Requests
- IT Help Desk
- IT Service Management Portal
- Technical Services
- IT Sentara eCare Health Network
- IT Security**
- IT Self Service Catalog
- Wavenet and Teamsites (Sharepoint) Information Center
- Enterprise Application Portal
- Sentara Telehealth
- Sentara Informatics Portal
- Think IT

Directories

- Business Unit Directory
- Spök Paging
- Physician Search

Resources

- Infection Prevention/Control
- Sentara Nursing
- Sentara MyChart
- Sentara Telehealth
- Traffic Map
- The Sentara Store

Announcements

OCTOBER MEANS...

- HALLOWEEN
- PUMPKIN SPICE LATTES
- CYBERSECURITY AWARENESS MONTH

STATSAFEDONLINE.ORG / CYBERSECURITY-AWARENESS-MONTH

Cybersecurity Training

Security Awareness Materials

- Cybersecurity at Work Tip Sheet
- Cybersecurity While Traveling Tip Sheet
- Identity Theft and Internet Scams Tip Sheet
- E-Skimming Tip Sheet
- Internet of Things Tip Sheet
- Multi-factor Authentication Tip Sheet
- Online Privacy Tip Sheet
- Passwords Tip Sheet
- Phishing Tip Sheet
- Protecting Your Digital Home Tip Sheet
- Social Media Cybersecurity Tip Sheet
- SANS: Security Awareness Work-from-Home Deployment Kit

LinkedIn Learning

- Cybersecurity at Work
- Inside the Breach
- The Internet of Things (IoT)
- Understand Threat Intelligence
- Phishing and Whaling
- Breaking Down Cloud Security
- Malware Explained
- Tips for Working Remotely
- Ethical Hacking: Social Engineering
- Learning Ransomware Countermeasures

National Cybersecurity Awareness Month

NCSAM Weekly Resources

- Cybersecure Your Smart Home Tip Sheet
- Cybersecure Your Smart Business Tip Sheet

Other Resources

Helpful Links

- US-Cert
- HHS Breach Reports

Hot Topics

- Global CISO 100 - 2020 Winners | Dan Bowden

Exceptions

- Submit a Security Exception Request
- Compliance 360



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](https://www.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.