

Cybersecurity : Malware Protection & Vulnerability Scanning and Assessment

Oregon Coast Community College
November 2022

Robin Gintner, VP of Administrative Services
Spencer Smith, Director of Information Technology

INFORMATION
TECHNOLOGY

@occcsharks



Table of Contents

- Phishing Activities
 - Image: Last 6 Months Phishing
- CISA: Cybersecurity and Infrastructure Security Agency
 - Image: Cyber Hygiene Report Card, 2022-11-02
- DarkTrace Incident Reporting and SOC
 - Image: DarkTrace .16 Subnet Display
- Questions?



Phishing Activities

- Email Phishing attacks: Barracuda
 - Dramatically Increased Activity (up 61% over 2021)
 - Spear Phishing (Targeted individuals or groups)
 - Site Spoofing (Links that aren't what they say they are)
- Phishing Testing and Training: KnowBe4
 - Weekly Phishing Test
 - Automated Training
 - Phone email can be problematic

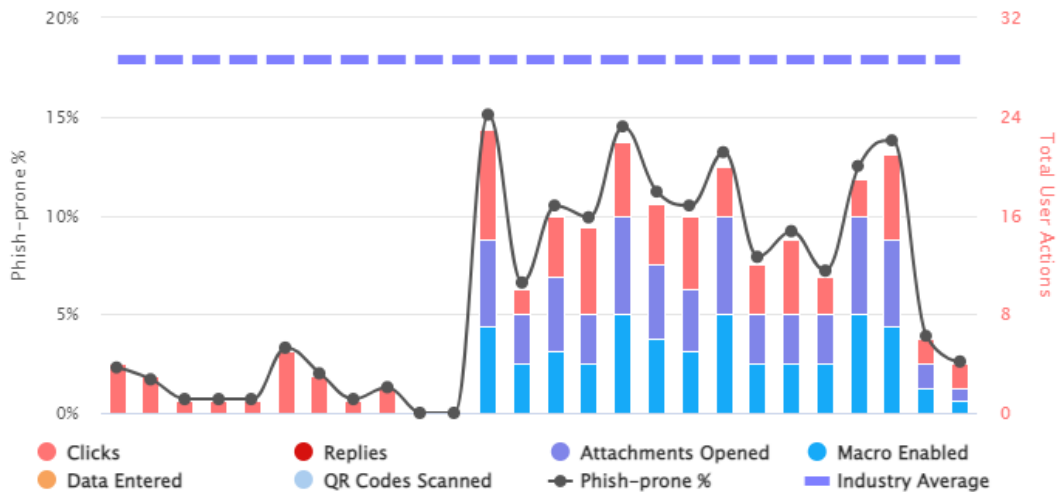


Phishing Activities, Last 6 Months

Phishing

Phishing Security Tests – Last 6 Months

92 Clicks, 0 Replies, 78 Attachments Opened, 77 Macro Enabled, 0 Data Entered, 0 QR Codes Scanned



Industry Benchmark Data ?

Account Average Phish-prone %	5%
Last Campaign Phish-prone %	2.6%
Industry Phish-prone %	17.9%

Industry: Education

Organization Size: Small (<250 user)

Program Maturity: 90 Day

Industry Benchmark Chart Data

CISA: Cybersecurity and Infrastructure Security Agency

- Free Service provided by the Federal Government
- Monthly Vulnerability Scanning
- Monthly Web Security Scanning
- Very Comprehensive Network Assessment

INFORMATION
TECHNOLOGY

@occcsharks



Cyber Hygiene Report Card, 2022-11-02

2022-11-01

CYBER HYGIENE

REPORT CARD

Oregon Coast Community College

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts





 **CISA**
CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

August 14, 2022 — November 2, 2022
Host Scans on All Addresses

November 1, 2022 — November 1, 2022
Vulnerability Scans on All Hosts

ADDRESSES OWNED	ADDRESSES SCANNED
8  No Change	8  No Change 100% of addresses scanned
HOSTS	SERVICES
1  No Change	2  No Change
VULNERABLE HOSTS	VULNERABILITIES
0  No Change 0% of hosts vulnerable	0  No Change

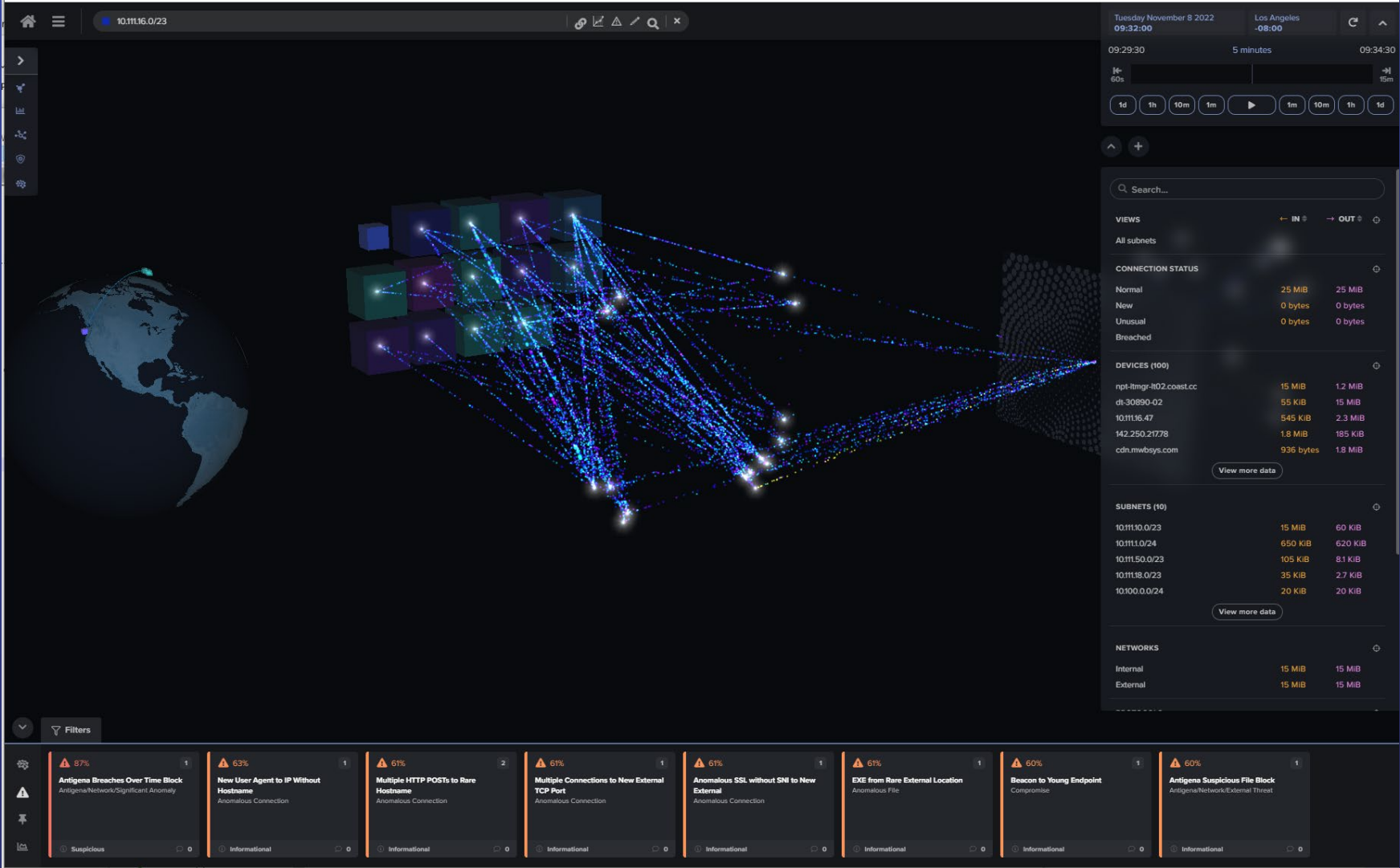
INFORMATION
TECHNOLOGY

DarkTrace: AI Security Operations Center

- On-premise device, linked to central DarkTrace service in the cloud
- Continual scanning of operational security
- Email Scanning
- Device Compliance



DarkTrace AI Security Operations Center



INFORMATION
TECHNOLOGY



INFORMATION TECHNOLOGY

Questions?

@occcsharks

