Philadelphia International Airport (PHL)
Northeast Philadelphia Airport (PNE)

Peter Yong

Information Security Group

City of Philadelphia,
Department of Aviation

2023-12-05

PHL PNE

PHILADELPHIA INTERNATIONAL AIRPORT
NORTHEAST PHILADELPHIA AIRPORT

Department of Aviation's Information Security Group

PHL PNE
PHILADELPHIA INTERNATIONAL AIRPORT
NORTHEAST PHILADELPHIA AIRPORT

Team Overview

Information Security Group

Who:

Peter Yong – Manager

Omotolani Etti – Engineer

Wayne Lawrence – Analyst

Where:

IP2 2nd Floor

Email: infosec@phl.org

Three Pillars of Information Security – C.I.A.

Confidentiality:

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy, proprietary and operational information

Integrity:

Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity

Availability:

Ensuring timely and reliable access to and use of information

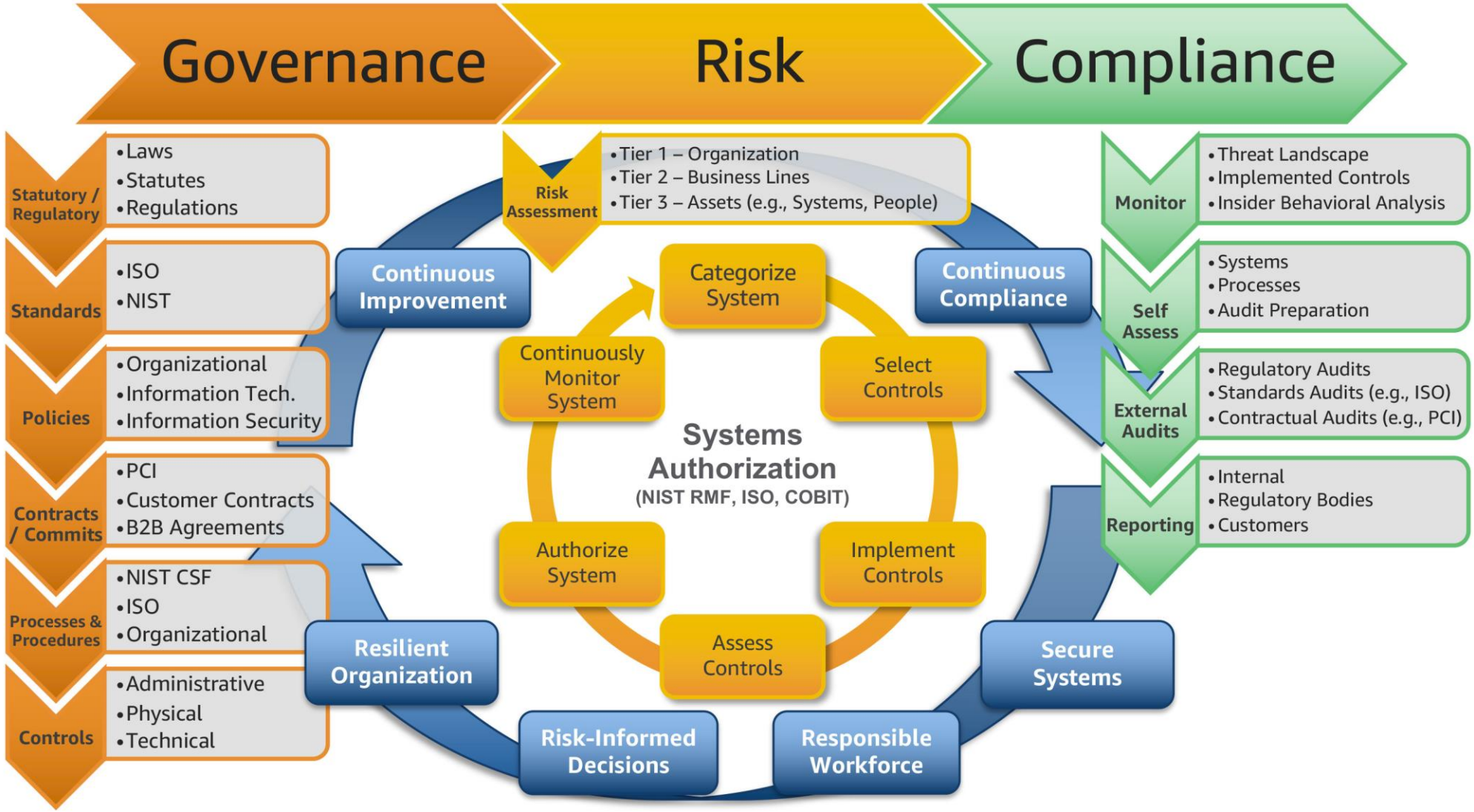
Why is DOA/PHL a target?

- Monetary gains
- Political
- Hacktivist
- Competitor
- Distraction
- Revenge
- Fame
- Just for fun! Hobby!

TOP Threats to DOA

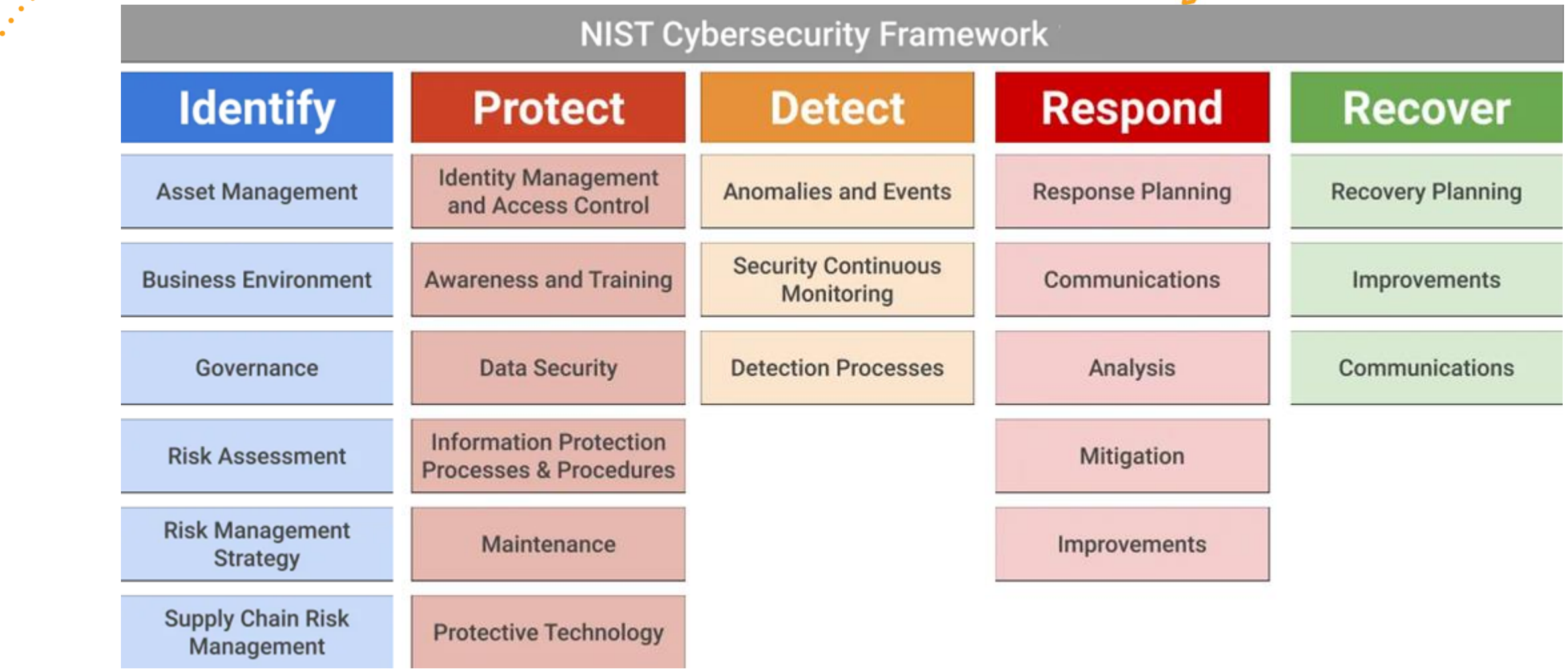
Social Engineering
DDoS – Denial of Service
Data Security
Vulnerabilities
Access Control
Internet of Things

Strategy to protect DOA



PHL PNE

NIST CSF and 800-53 Framework



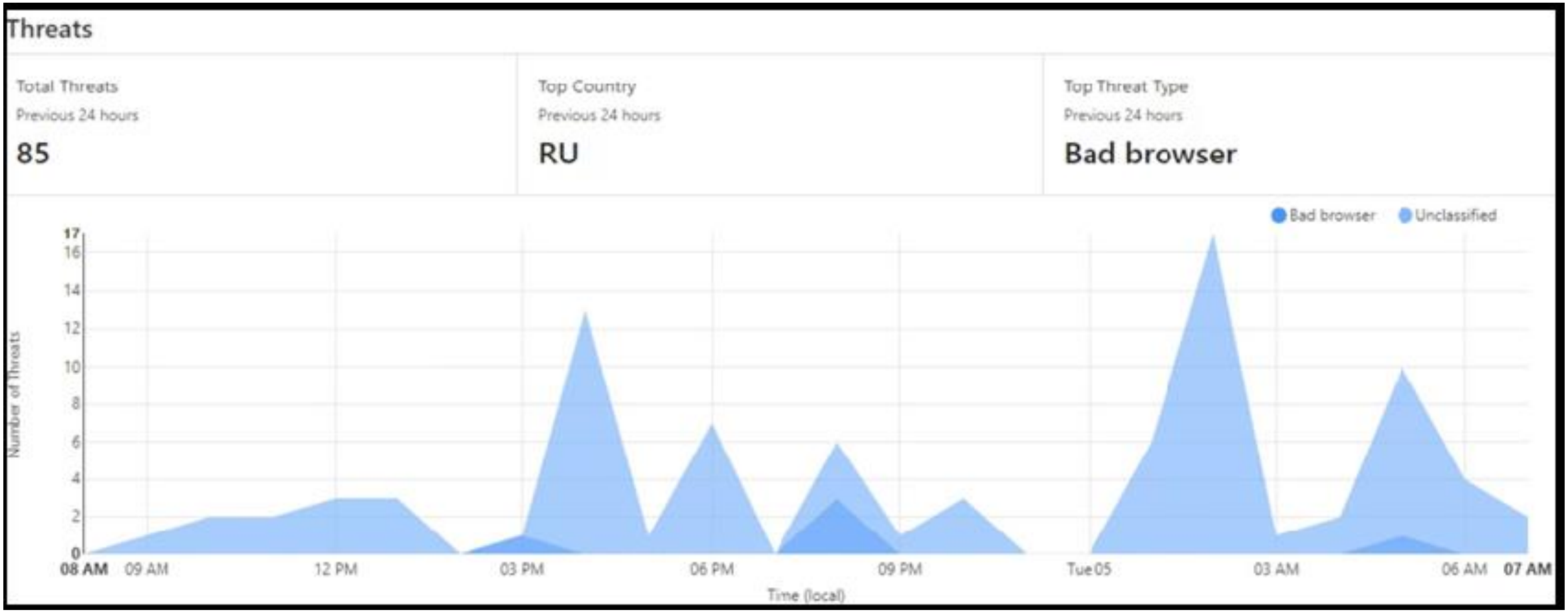
Highlights

Awareness Training Program
Multifactor Authentication (MFA)
Incident Response Plan
Third party Risk Management Program
Mobile Device Protection (PHL iPhones)
Endpoint protection (Falcon and Umbrella)
USB Drive Security
Cybersecurity Awareness Month
Monitoring of network traffic in/out of PHL for malicious activities
Completed first pen test on PHL network assets
Cyber Hygiene WebApp Scanning

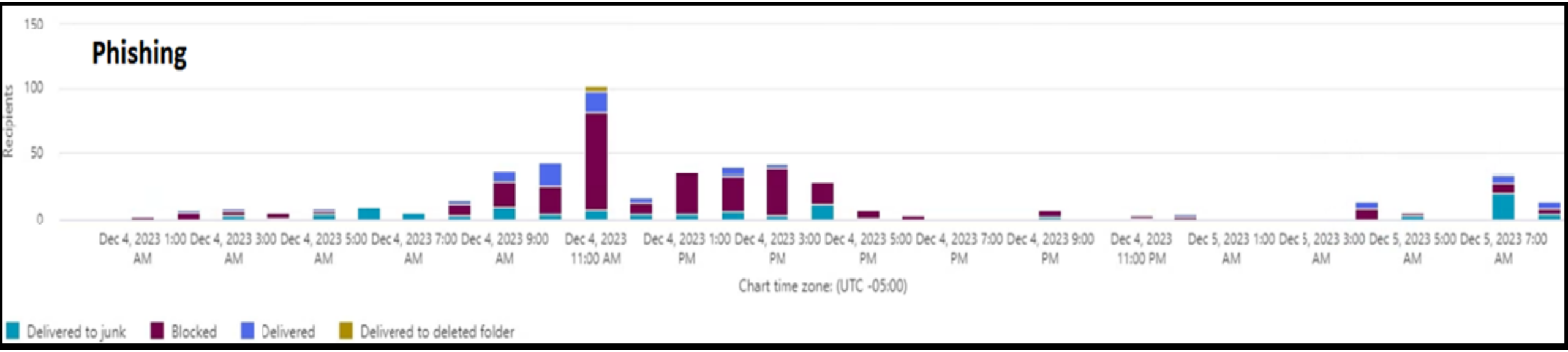
Cybersecurity Awareness Month

PHL PNE

Threats we observe daily



Threats we observe daily

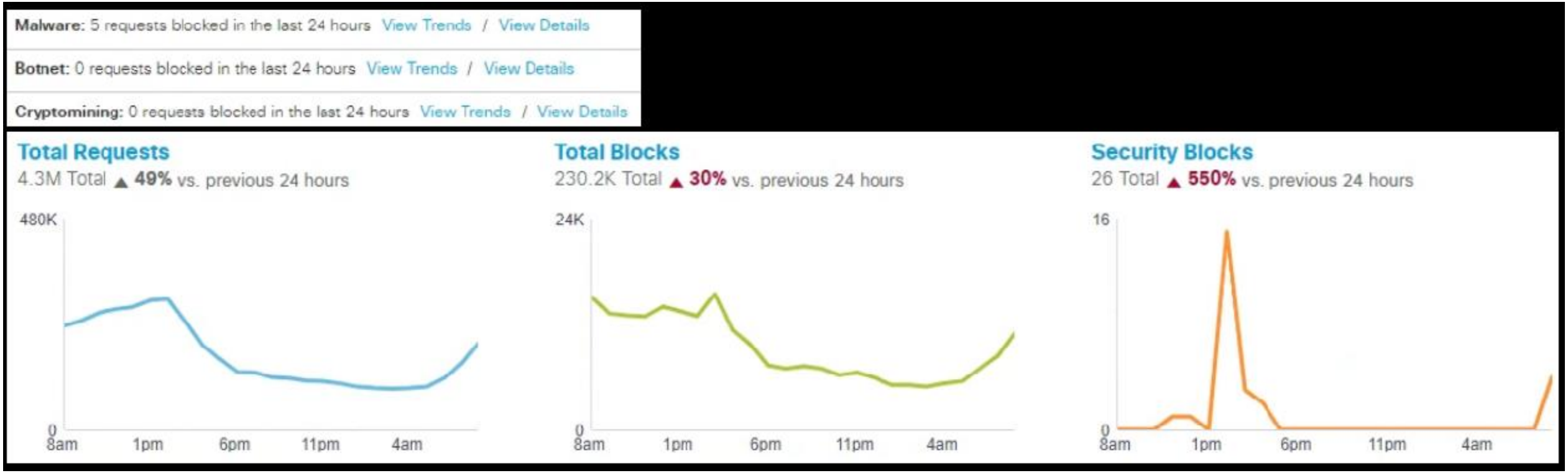


Threats we observe daily

Malware: 5 requests blocked in the last 24 hours View Trends / View Details

Botnet: 0 requests blocked in the last 24 hours View Trends / View Details

Cryptomining: 0 requests blocked in the last 24 hours View Trends / View Details



PHL PNE

Threats we observe daily

Login Activity

OFFICE 365

Last 24 hours | Hide Filters

Login Failures

Login Failures

_time	User	LogonError	Client IP
2023-12-05 09:02:20	Not Available	UserStrongAuthClientAuthNRequiredInterrupt	2601:8c:97e:7610:e5ca:d74e:e879
2023-12-05 09:02:19	Meg[redacted]	.org	UserStrongAuthClientAuthNRequiredInterrupt	2601:8c:97e:7610:e5ca:d74e:e879
2023-12-05 09:01:39	Mil[redacted]	l.org	IdsLocked	114.104.158.172
2023-12-05 09:01:39	Mil[redacted]	l.org	IdsLocked	114.104.158.172
2023-12-05 09:01:16	Mil[redacted]	l.org	IdsLocked	183.237.243.50
2023-12-05 09:01:15	Mil[redacted]	l.org	IdsLocked	183.237.243.50
2023-12-05 09:01:15	Mil[redacted]	l.org	IdsLocked	183.237.243.50
2023-12-05 09:00:57	Mil[redacted]	l.org	IdsLocked	221.10.71.234
2023-12-05 09:00:57	Mil[redacted]	l.org	IdsLocked	221.10.71.234
2023-12-05 09:00:57	Mil[redacted]	l.org	IdsLocked	221.10.71.234

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Geographical Improbable Access

Users logging in at two different locations where it's not likely possible to travel between locations in the time specified

UserId	Day	Time Difference (H)	Distance (M)	Speed	Original Location	Original Source IP	Second Location	Last Source IP
Not Available	12/05/2023	3.51	13594.57	3873.10	Chennai, India, Tamil Nadu	100.14.154.27	Philadelphia, United States, Pennsylvania	182.72.70.196
Not Available	12/05/2023	0.67	13594.39	20290.14	Philadelphia (Center City), United States, Pennsylvania	182.72.70.196	Chennai, India, Tamil Nadu	192.82.102.253
Not Available	12/04/2023	0.14	13480.63	96290.24	Navi Mumbai (Reliance Corporate Park), India, Maharashtra	198.91.10.13	Greenwood Village, United States, Colorado	2409:4072:987:c600:212c:7979:af0f:bd8a

PHL PNE

Successes in preventing attacks

- Fended off DDoS attacks in August 2023
- Fended off pen test (endpoints and servers)
- Detected and removed endpoint malicious apps

Impact on the Department of Aviation's Mission & Vision

Vision — We are a World Class Global Gateway of Choice

Mission — Proudly Connecting Philadelphia with the World

- Provides clear direction on standards and procedures:
  - Facilitates the confidentiality, integrity, and availability of data
  - Reduces the risk of security incidents
  - Executes security programs across an organization
  - Provides clear statement of security policy to third parties
  - Helps to address regulatory compliance requirements, e.g. HIPAA, TSA, CISA

Collaboration

All business units

Information Technology

TSA and CISA

Airlines

Third party vendors

Continuing Information Security Work

Threat landscape constantly changes day to day

Staying up to date with ongoing threats and vulnerabilities

Working through our Information Security Programs

Q & A

Thank You!

Peter Yong

infosec@phl.org

City of Philadelphia,
Department of Aviation

PHL PNE

PHILADELPHIA INTERNATIONAL AIRPORT
NORTHEAST PHILADELPHIA AIRPORT