

Transformational Innovations & Cybersecurity

JOE TENGA

*CHIEF INFORMATION OFFICER
JACKSONVILLE TRANSPORTATION AUTHORITY
JACKSONVILLE, FL*

Latest Innovation Trends

- Artificial Intelligence
 - Facial Recognition
 - Lip Reading
 - Chatbots
 - Threat Defense & Response
- Blockchain
- Autonomous Vehicles
- Connected Devices & IoT
- 5G Wireless
- Augmented Reality
- 3D Printing

The Workforce of Tomorrow

START PREPARING TODAY

HELP WANTED

Connected Devices

IoT

Marketing

Autonomous Vehicles

Cybersecurity

Data Science

Software Development

State of Cyber Security 2017

Workforce Trends and Challenges

ISACA's third annual State of Cyber Security study finds that the field remains dynamic and turbulent during its formative years. One of the core challenges remains the persistent cyber security skills gap, and the difficulty of finding qualified candidates to fill cyber security positions. Security leaders share their workforce observations and challenges in the findings below. Get more workforce-related data and implications at www.isaca.org/state-of-cyber-security-2017.

Hiring Challenges Persist

55%



indicate that open positions take at least **THREE MONTHS** TO FILL.



32%

OF ENTERPRISES

report that the time to fill cyber security and information security positions is **SIX MONTHS OR MORE**.

MORE THAN

1 IN 5

organizations get **FEWER THAN 5 APPLICANTS** for an open cyber security position.



ONLY 13%

GET 20 OR MORE APPLICANTS.

HIRING STATUS

Many are **UNABLE TO FILL** open cyber security positions in their enterprises:

IN THE US:

59%

CAN FILL OPENINGS

14%

DON'T KNOW



Skills and Certifications in Demand

37%



SAY **FEWER THAN 1 IN 4** candidates are qualified

55%

SAY **PRACTICAL HANDS-ON EXPERIENCE** is the most important qualification for a cyber security candidate.



CLOSE TO

70%

of hiring enterprises require a **SECURITY CERTIFICATION** for open cyber security positions.



The Trouble with Talent

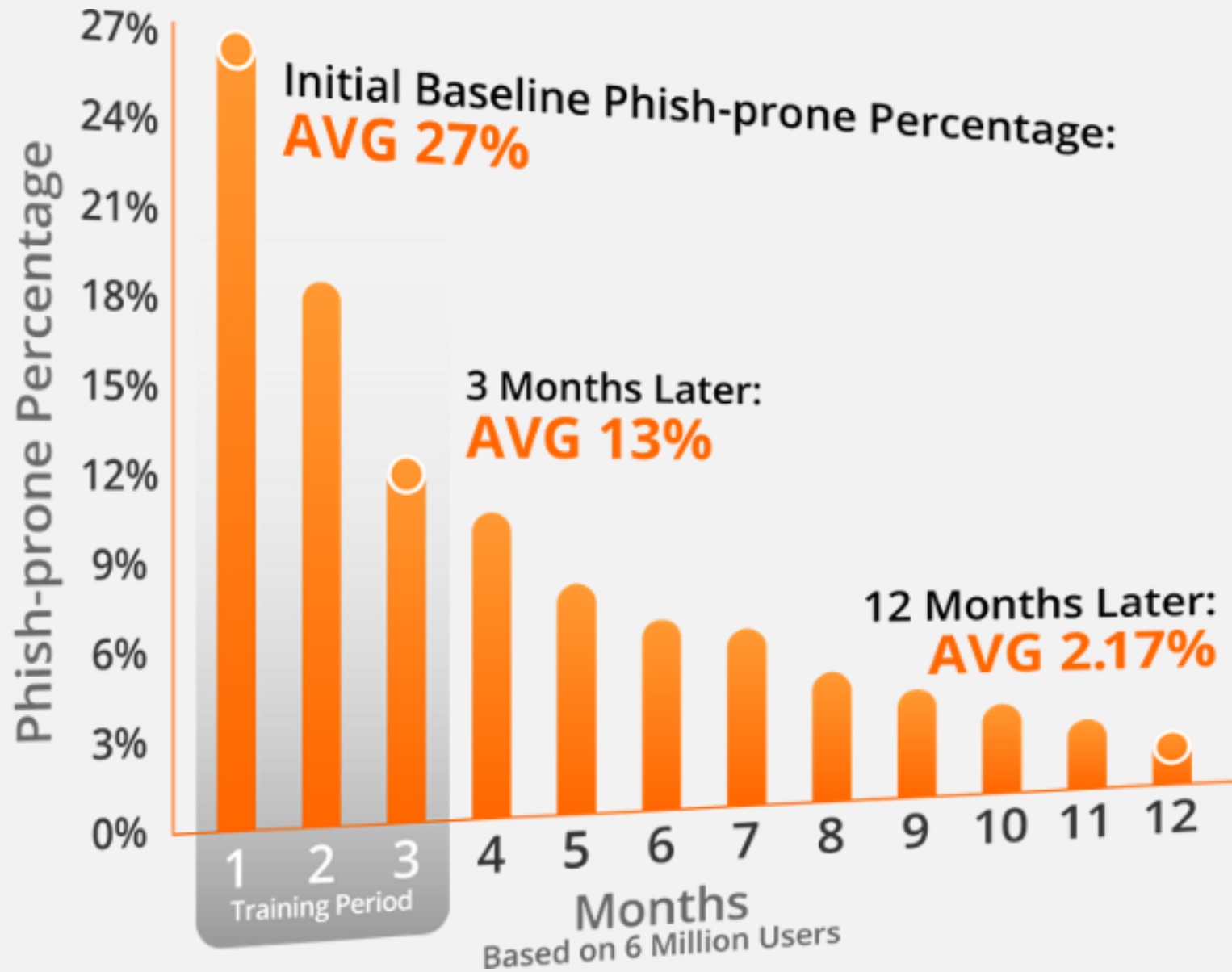
GROWTH INHIBITORS

- Availability of qualified talent
- Cost of highly skilled workers
- Resistance to Change

JTA University Training Roadmap

- ✓ **Computer Based Training (CBT)**
- ✓ **Security Awareness Training**
- ✓ **Augmented Reality**
- ✓ **Mentoring & Reverse Mentoring**
- ✓ **Mock Phishing Campaigns**















BE PREPARED.

**FIGHT PHISHING
WITH PHISHING!**

My Inbox... three weeks ago

	FROM	SUBJECT
	Matthew Connard	IT Scorecard Deadline
	Emma Rouhana	Parking Passes for Downtown Garage
	Randy W. Brewer	RE: Project Reconciliation
	SolarWinds	Win prizes learning about the newest SolarWinds products
	Denise Martinez LaPorte	Orgchart_31418.docx
	Nathaniel P. Ford	Read the latest news on transport security and safety
	Nathaniel P. Ford	Do you have a resignation letter prepared?
	Mary O'Mahoney	RE: Joe Tenga Bio for APTA profile
	Trapeze Group	Reminder: Please Tell Us How We Can Improve!

Gartner CIO Leadership Forum
Forum 2018

25 – 27 March 2018 / Hollywood, FL



Gartner.

CIO Leadership Forum

Seven Reasons More CEOs Will Be Fired Over Cybersecurity Breaches and How To Ensure Yours is Not Next

Paul E. Proctor
@peproctor

CYBERSECURITY MATURITY

ROLES AND RULES

BOARD OF
DIRECTORS



CEO

CIO & IT

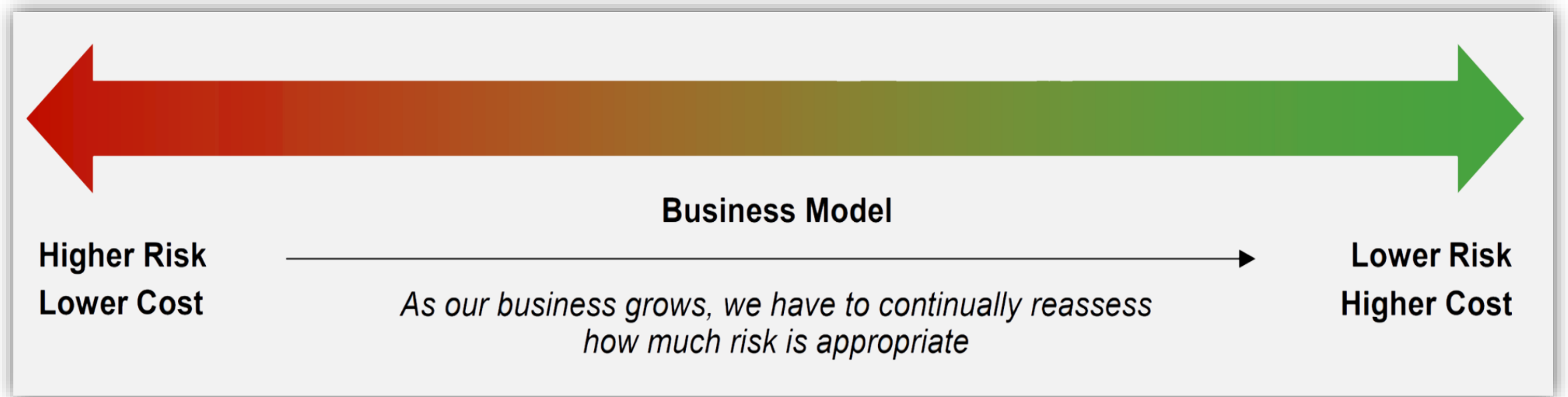


END USERS

Cybersecurity = Enterprise Risk Management



“What will it cost to make our Agency secure?”



Less Secure

More Secure

RULE #1

Don't execute someone else's Cyber-Strategy!



- Yes. Vendors sell useful products
- Moderate Board, Executive and IT reactions to media hype
- Prioritize strategic security initiatives based on Risk and Data

RULE #2

Don't buy new Security toys unless you already...

- Regularly patch servers/desktops
- Changed vendor default passwords
- Enforce strong user authentication (passwords, MFA)
- Removed unsupported Operating Systems (like WinXP)
- Revoked Local Administrator privileges from end users

These steps avoid between 80-90% of all breaches

RULE #3

Get with the Security Program

- Security standards promote best practices
- Implement Controls and Procedures to experience a sharp increase in maturity
- Again, not just IT, this is an **Enterprise** concern
- Identify legal and professional mandates
- NIST CSF at a minimum (PCI-DSS, HIPAA, etc)

JTA's Cybersecurity Program: Smarter not Harder

- NIST 800-53
- NIST 800-171
- NIST CYBERSECURITY FRAMEWORK
- NISPOM
- DFARS 252.204-7012
- FAR 52.204-21
- FEDRAMP
- FACTA
- FINRA
- ISO 27002
- ISO 27018
- GAPP
- PCI DSS
- COBIT 5
- HIPAA
- SOX
- GLBA
- NY DFS 23 NYCCRR 500
- AICPA SOC2
- CIS CSC
- CSA CCM
- ENISA
- EU GDPR
- UK DPA
- MASSACHUSETTS 201 CMR 17
- OREGON 646A

The selected toolkit provides Policy statements, associated Standards, Controls, Key Performance Indicators, Key Risk Indicators and a cross walk of all the above listed Security Frameworks

A Change of Perspective

CYBER-THREATS, THE NETWORK PERIMETER
& WHAT JTA IS DOING ABOUT IT

Cyber-Espionage: 2017 Statistics



- Constitutes 21% of all breaches
- Most common form of attack across multiple industries
- More than 90% of confirmed breaches attributable to state-affiliated groups

Complacent Consumers



Cyber-Terrorism

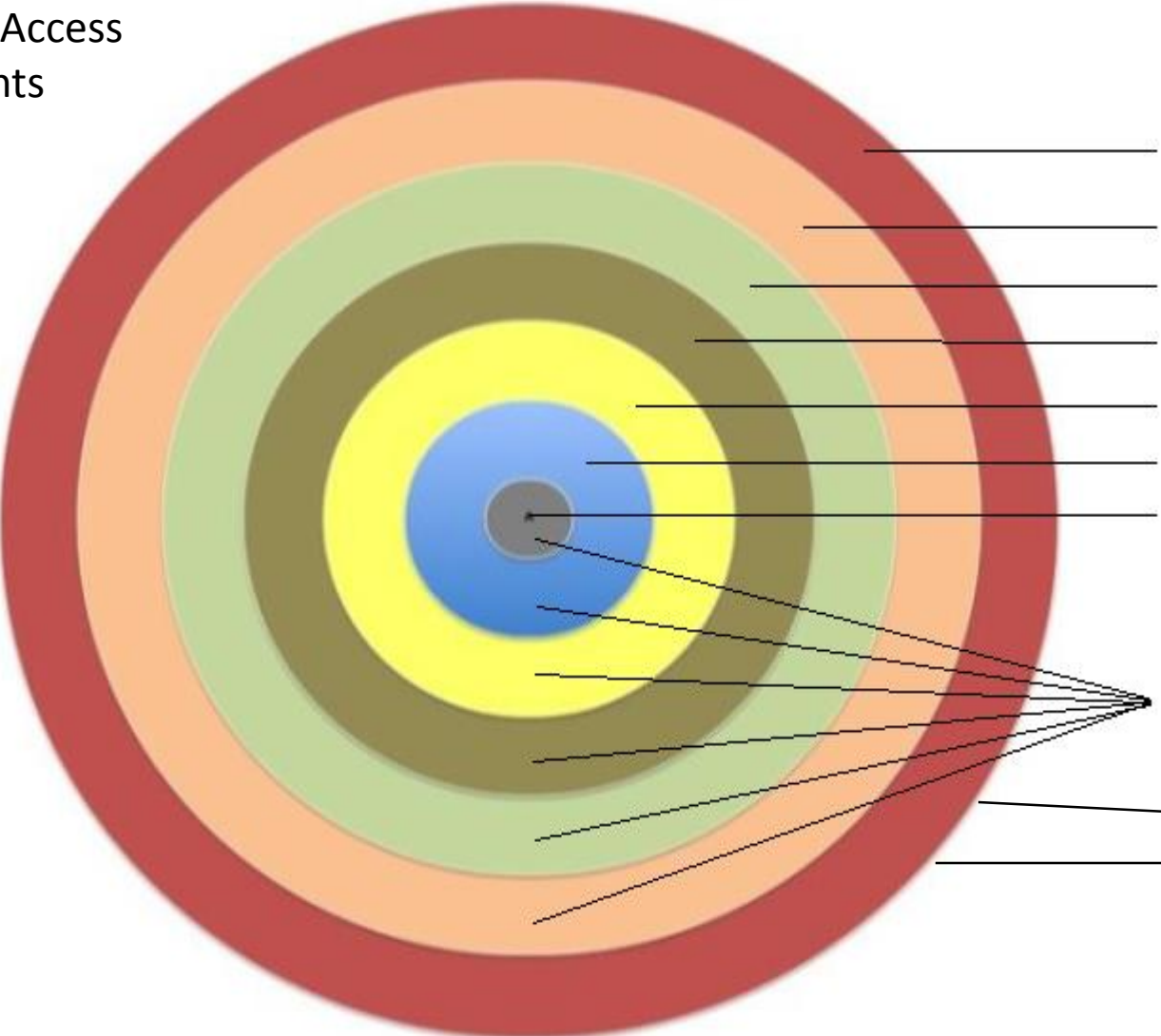


Unnamed petrochemical plant in Saudi Arabia, Aug 2017

The Traditional Network Security Perimeter

is not enough!

- Software as a Service Apps
- Business Partner Access
- Cloud Deployments
- Remote Workers
- Mobile Devices
- Outsourced IT
- IoT Devices



Intrusion Detection/Prevention

Firewall Protection

Email Scanning/Spam Filtering

Web Content Filtering

Anti-virus/Anti-malware

Patch Management

System Hardening

Internal Vulnerability Scanning

External Vulnerability Scanning

External Penetration Testing

Policy & Procedure

Identity is
the last(?)
Security
Perimeter

SO...

NOW

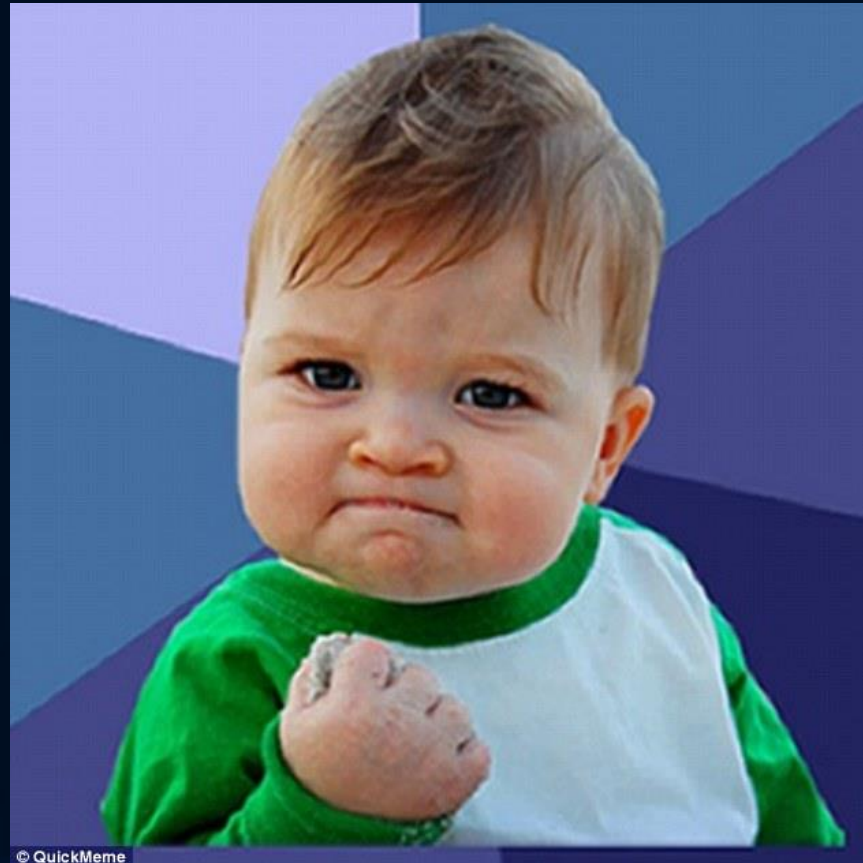
WHAT?

“Enterprise Defense” Shopping List

- Reliable defense from zero-day malware
- Real-time threat detection
- Unattended threat mitigation
- Protection from Technological Obsolescence
- Defends IT, IoT, ITS, Cloud and SaaS
- Detects Internal, External, and Colluding Threat Actors
- Detects compromised Identity and Privilege escalations





CHALLENGE ACCEPTED







Dashboard

 **Running Threats**
0
Total

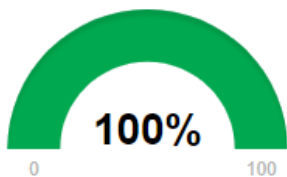
 **Auto-Run Threats**
0
Total

 **Quarantined Threats**
453
Total

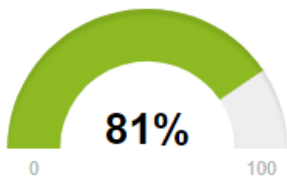
 **Unique**
0
Total

Total Files Analyzed
29,743,947

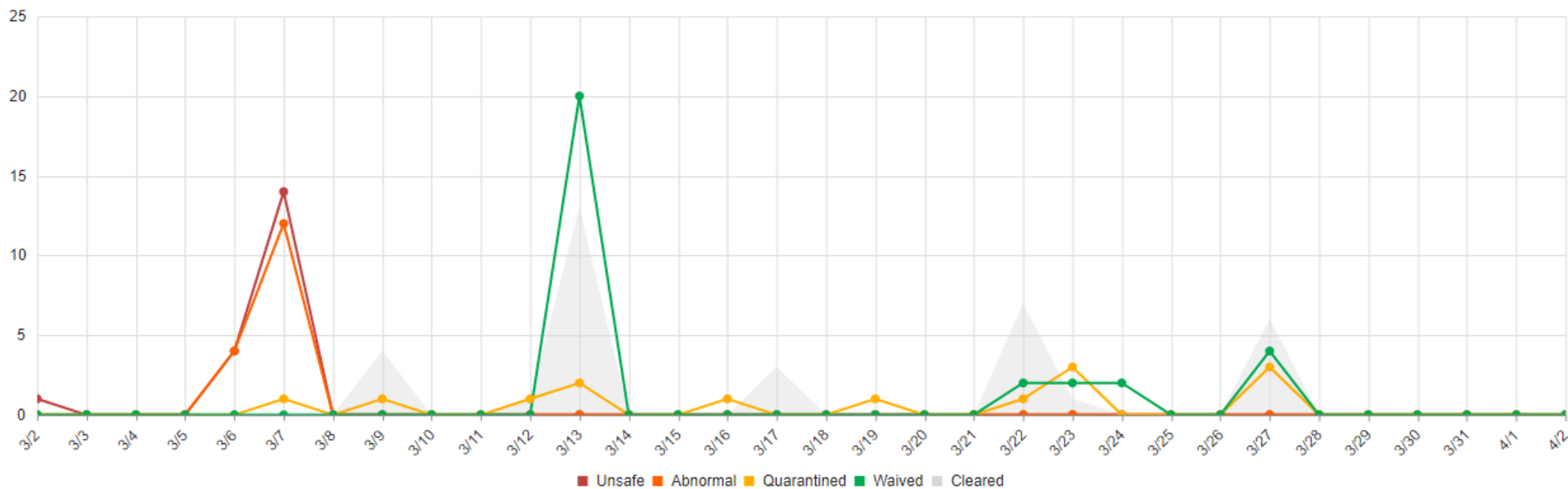
Threat Protection



Device Protection



Threat Events



Threats By Priority

Total

0

Threat Classifications

Malware

Trojan

Backdoor

PUP

Adware

Hacking Tool

Top Ten Lists

THREATS

DEVICES

ZONES

Threats found on the most devices

JTA's A.I. Anti-Malware Selection

- ✓ Reliable defense from zero-day malware
- ✓ Real-time threat detection
- ✓ Unattended threat mitigation
- ✓ Protection from Technological Obsolescence
- ❑ Defends IT, IoT, ITS, Cloud and SaaS
- ❑ Detects Internal, External, and Colluding Threat Actors
- ❑ Detects compromised Identity and Privilege escalations

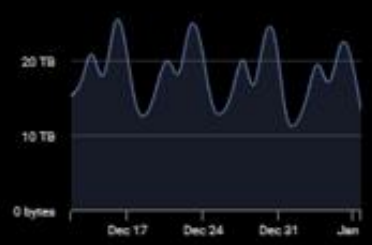


CURRENTLY ANALYZING

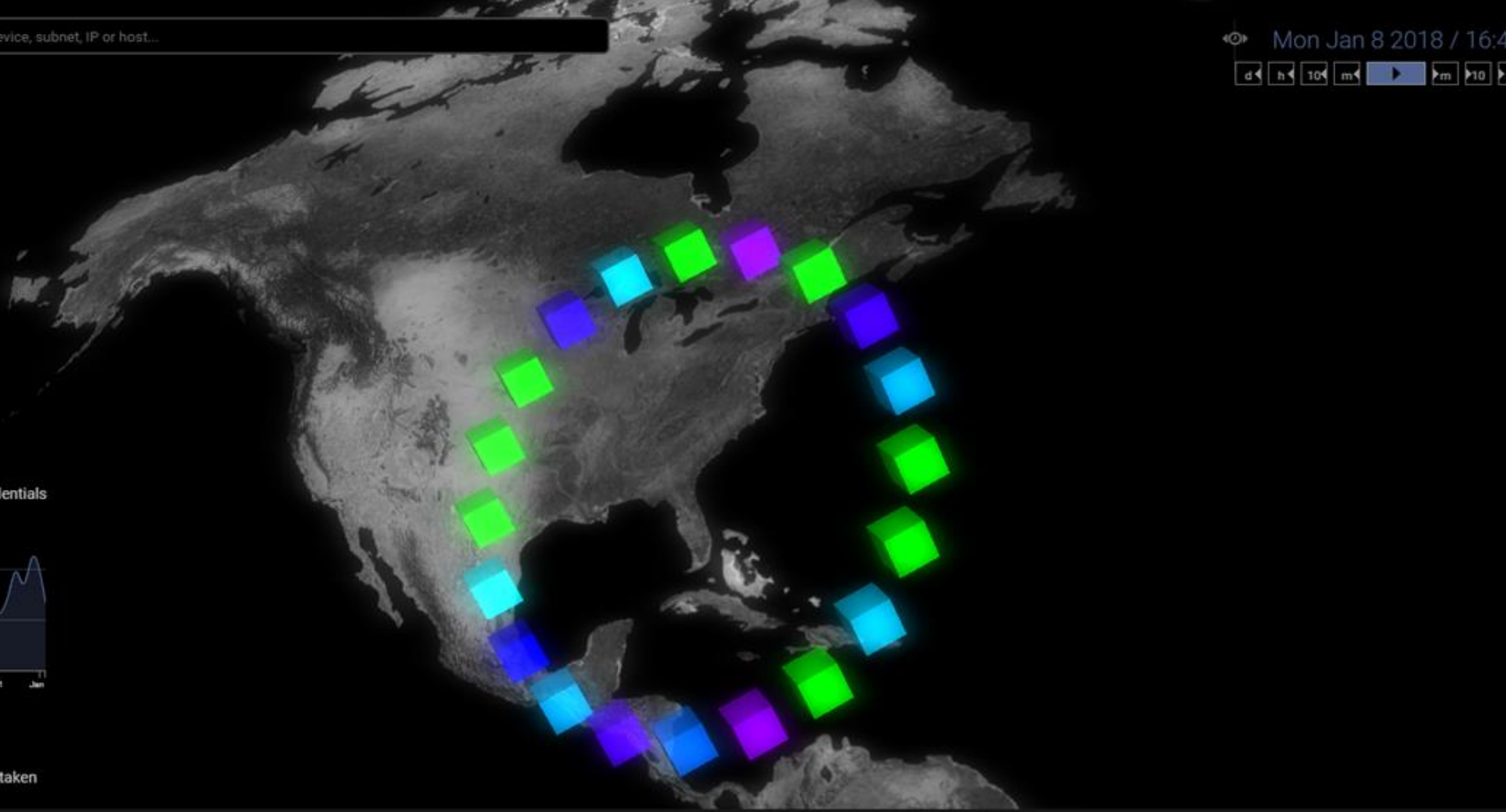
926,180 patterns of life

67 subnets 1,967 devices

486 servers 1,481 clients 2,036 user credentials



264 controlled devices 3,955 actions taken



3 [redacted] age01. jtafl.com	2 [redacted] cd01. jtafl.com	2 [redacted] lgf01. jtafl.com	2 [redacted] sfl.com	7 [redacted] po1. jtafl.com	4 [redacted] in. jtafl.com	6 [redacted] /	3 [redacted] l. jtafl.com	2 iPhone	2 [redacted] l. jtafl.com	9 [redacted] nai.net	2 [redacted] .com	4 [redacted]
-------------------------------------	------------------------------------	-------------------------------------	-------------------------	-----------------------------------	----------------------------------	-------------------	---------------------------------	-------------	---------------------------------	-------------------------	----------------------	-----------------

JTA's A.I. Enterprise Defense Selection

- ✓ Reliable defense from zero-day malware
- ✓ Real-time threat detection
- ✓ Unattended threat mitigation
- ✓ Protection from Technological Obsolescence
- ✓ Defends IT, IoT, ITS, Cloud and SaaS
- ✓ Detects Internal, External, and Colluding Threat Actors
- ✓ Detects compromised Identity and Privilege escalations



TRANSFORMATION IS HARD

- Innovation creates Cyber threats AND opportunities
- Get prepared... change is coming fast
- Everyone.. know your Roles & the Rules
- Understand your current threats and bad actors
- Don't be complacent... we're all counting on you.

The background features a dark blue field on the left that transitions into a series of curved, overlapping lines on the right. These lines form a tunnel-like perspective, with a grid of fine lines visible on the inner surfaces, creating a sense of depth and movement.

THANK YOU

JOE TENGA
CHIEF INFORMATION OFFICER
JACKSONVILLE TRANSPORTATION AUTHORITY