MAT-SU BOROUGH

Cyber Security Update

AML – AGFOA
Nov 19, 2019

Eric Wyatt
IT Director
Chief Information Officer
907-861-8570

Agenda

- Understand
- Prepare
- Partner

Understand the What

Ryuk

Dridex

Kovter

Brambul

NanoCore

TFlower

ZeuS

Living Off the Land

Gh0st

Cerber

Trickbot

WannaCry

CoinMiner

“If you’re asking me if I think we’re at war, I think I’d say ‘yes’…We’re at war right now in cyberspace. We’ve been at war for maybe a decade. They’re pouring oil over the castle walls every day.” — Gen. Robert Neller, Commandant, USMC, 21 February 2019

Counties Are on the Front Lines of Cyber War

USA
CYBER WARFARE
BUDGET INCREASE
+1200%

CHINA
CYBER WARFARE
BUDGET INCREASE
+1100%

SAM SPRATT - GIZMODO

Retired four-star Marine Gen. John Allen has seen the cyber threat in action and believes it's targeted at counties.

www.routefifty.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

www.csis.org

September 2018. The U.S. State Department suffers a breach of one of its unclassified email systems, exposing the personal information of several hundred employees.

September 2018. Researchers report that 36 different governments deployed Pegasus spyware against targets in at least 45 countries, including the U.S., France, Canada, and the UK.

October 2018. The U.S. Department of Homeland Security announces that it has detected a growing volume of cyber activity targeting election infrastructure in the U.S. ahead of the 2018 midterm elections.

December 2018. U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.

February 2019. U.S. Cybercommand revealed that during the 2018 U.S. midterm elections, it had blocked internet access to the Internet Research Agency, a Russian company involved in information operations against the U.S. during the 2016 presidential election.

March 2019. U.S. officials reported that at least 27 universities in the U.S. had been targeted by Chinese hackers as part of a campaign to steal research on naval technologies.

June 2019. U.S. grid regulator NERC issued a warning that a major hacking group with suspected Russian ties was conducting reconnaissance into the networks of electrical utilities.

Baltimore Florida Texas

12,449 breaches and leaks last year, a 424% increase on 2017

www.infosecurity-magazine.com

"Government was the largest growing exposed sector in 2018, increasing over 291% from 2018"

4iQ co-founder and CTO Julio Casal

Cybersecurity Ventures predicts that newly reported zero-day exploits will rise from one-per-week in 2015 to one-per-day by 2021.

Understand the Why

On Our Side

Staffing

Funding

Priorities

Complacency

What They Want

Data Gathering

Disruption

Ransom

Organizational Challenges

$$ Funding $$ ⇨ Bad guys easily out spend us

Lack of dedicated cyber security personnel

Learning new security tools

We need vendor support
- Managed Security Service Providers
- Market is evolving - Confusing - Fear - Snake Oil

We need partnerships with Federal, State, and other local governments

Government CIOs need to understand that adaptive security is a top technology trend this year.

Gartner

Challenges to our environment:

- **Culture** – Tend to be stable, cautious and risk-averse

- **Policies** - Rooted in data, impact studies, public debates and industry outreach

- **Processes** - Often-arcane government budgeting and acquisition

- **Tools** - Technical debt cripples most government agencies and hinders their ability to adopt emerging tools

- **People** - Skills imbalance, as well as personnel shortages

Understand Your Environment

Who Owns Information Security ?

We **ALL** do !

- Know Your Information
- Know Compliance rules: PII, PCI, HIPAA
- Know the threats
- Support the Information Security Policies

All personnel must understand security for the systems / processes they support and use

Understand the How

- Front door is locked

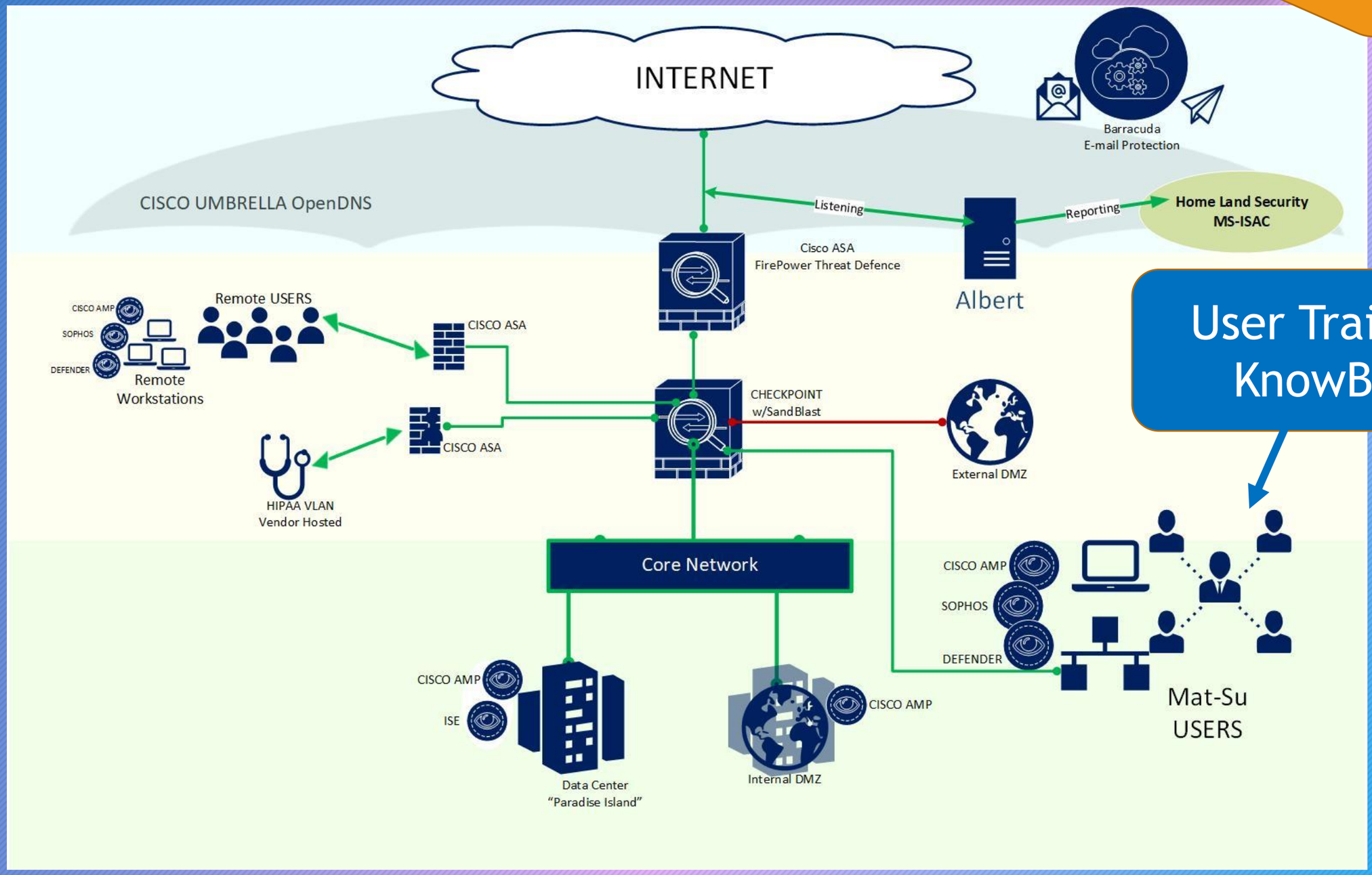
- Backdoor
  - Email Phishing & Web site malware

  - Smaller softer targets (**Local Governments**)
    - work their way up

  - Know your supply chain

MSB Current Posture
Nov 2019

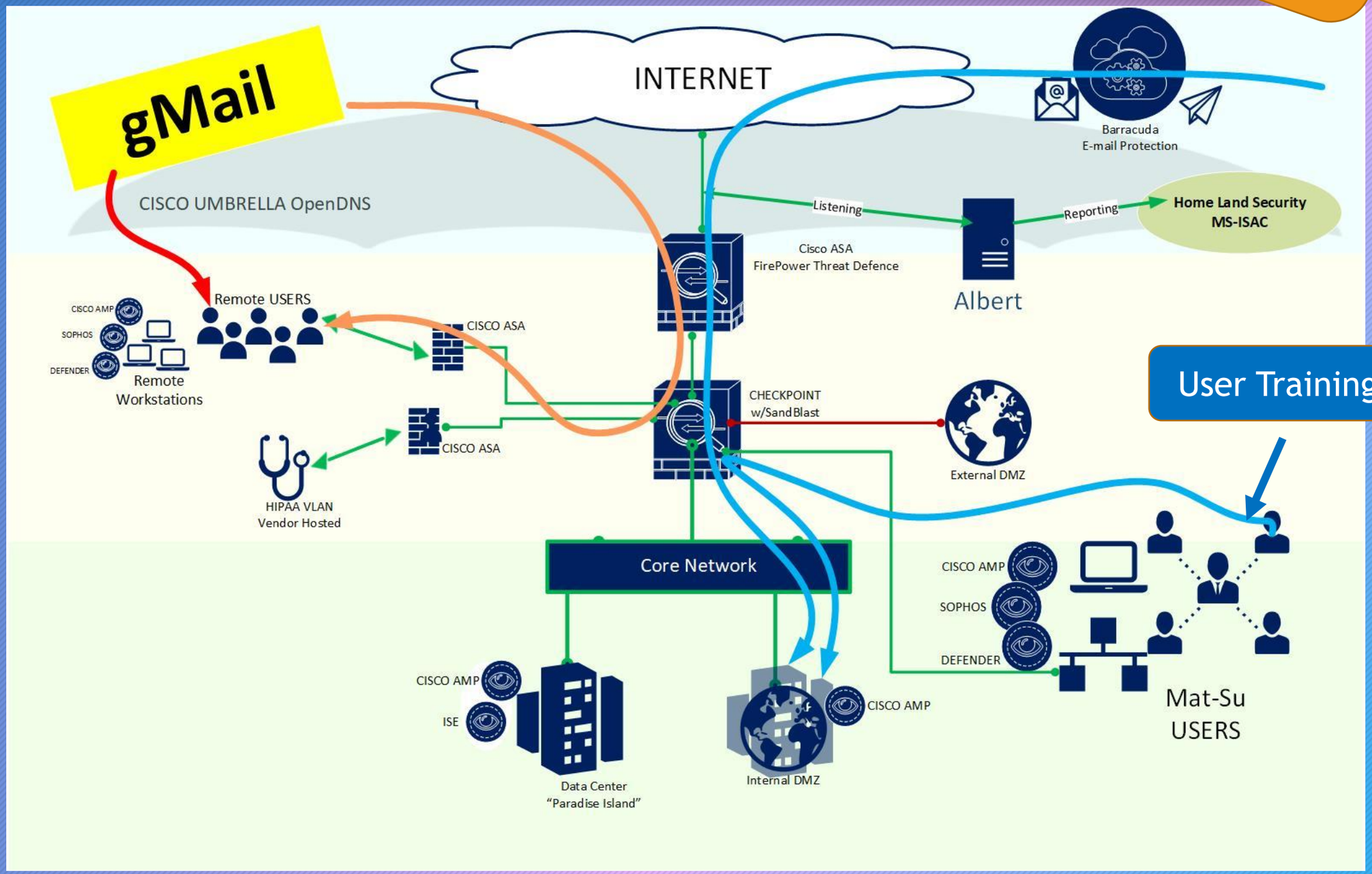
Understand
Prepare



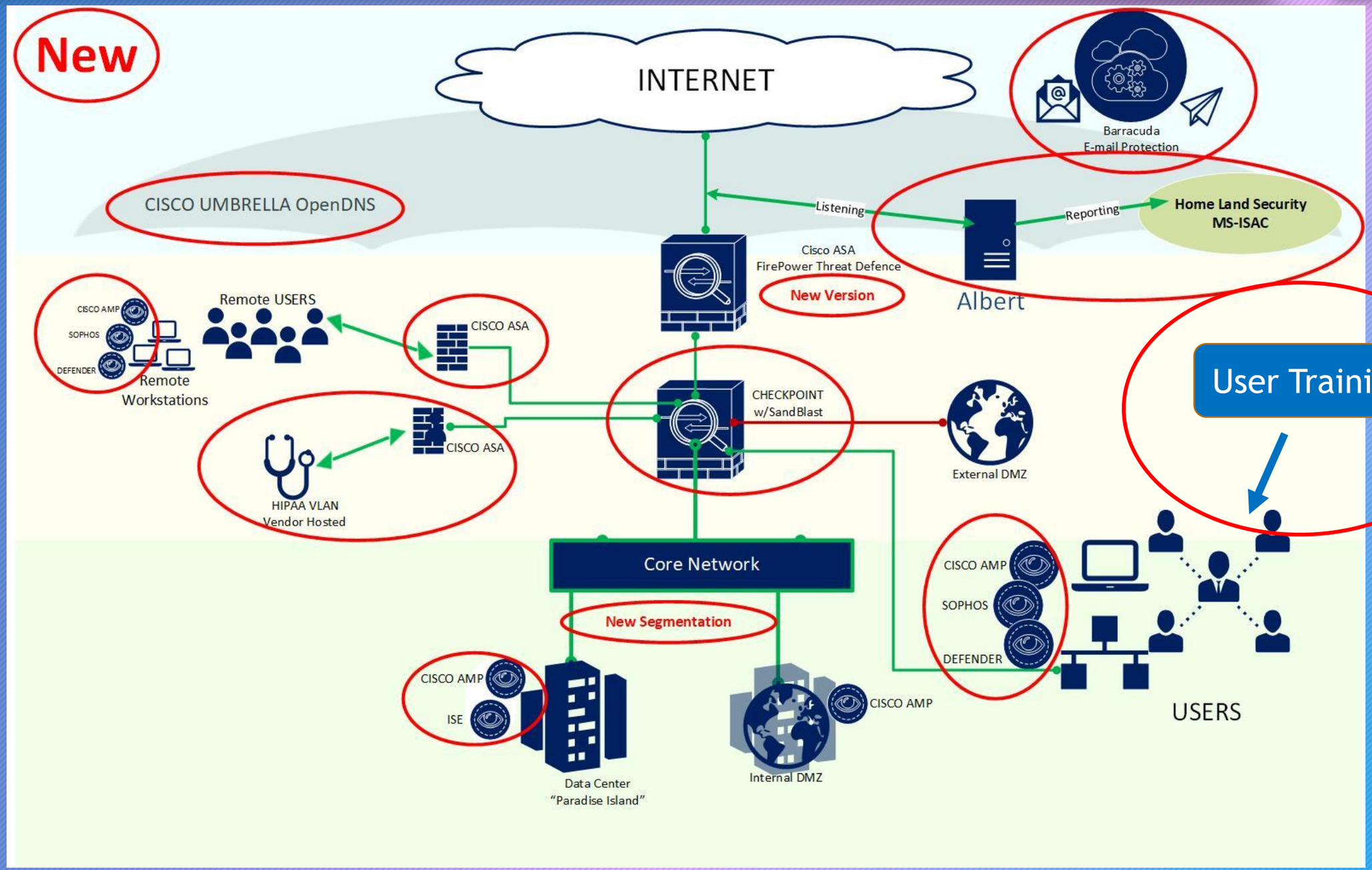
User Training
KnowBe4

Understand Prepare

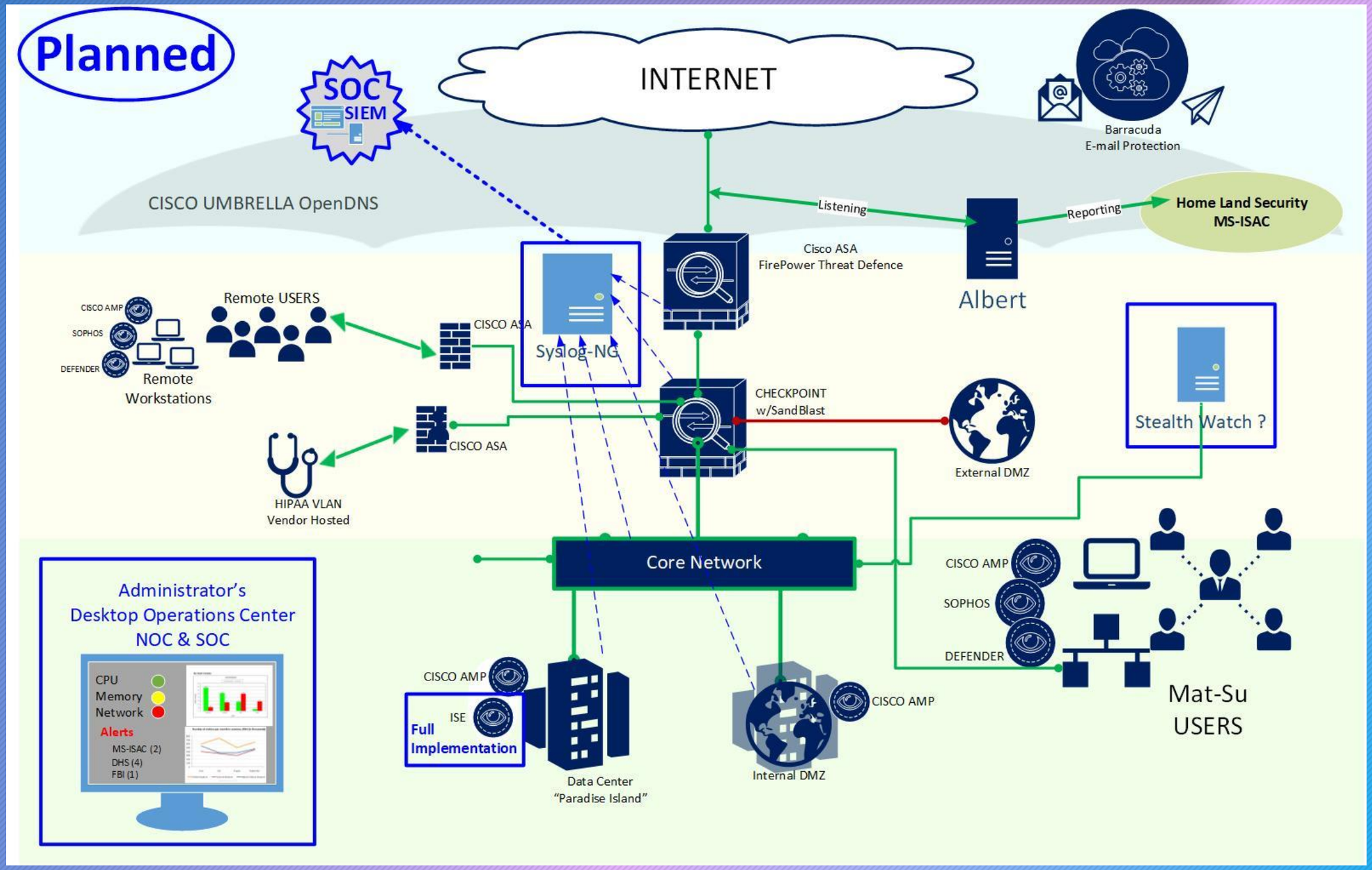
Use Cases
Data Flow



MSB Posture New Since Attack
Nov 2019



MSB Planned Posture
Nov 2019



Prepare

User Training

- Initial Phishing Champaign tests – User fails: 28%
- After Training – User Fails: 2%

Respond
~ Incident Response Plans

Public Relations

Vendors

Volunteers

Response Teams

Cyber Insurance

Emergency funding

Incident Command System (ICS)
Emergency Operations Center (EOC)

Communication

Communication

COMMUNICATION

Practice Makes Perfect

- Continuity Of Operations Plans
  - Practice an outage
- Disaster Recovery site / systems
  - Practice a switch over
- Off-line Backups
  - Practice Restores

Partnering

We Can't Do This Alone

DHS – MS-ISAC

InfraGard

AML

CIO Council

Smart Community Forum

Federal

State

Local

Commercial

Communicate…Communicate…Communicate

MS-ISAC

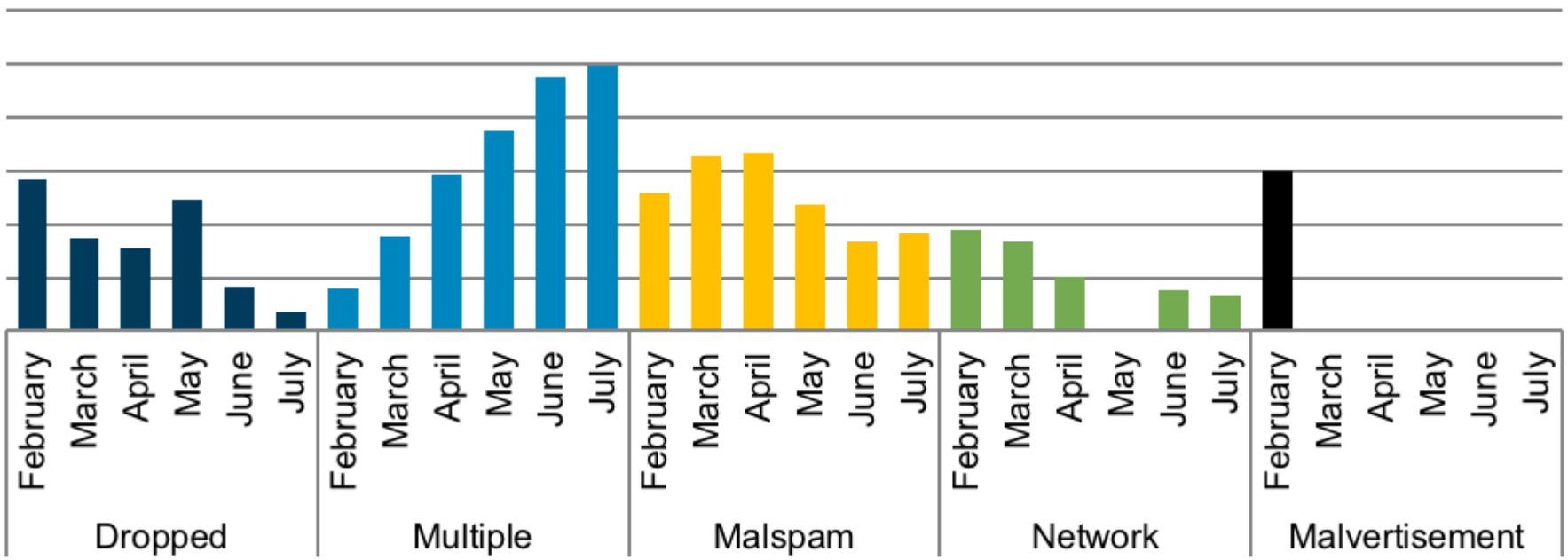
CIS Center for Internet Security®

Multi-State Information Sharing & Analysis Center

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Best Practices
Tools
Alterts

Top 10 Malware - Initial Infection Vectors TLP: WHITE



Dropped – Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a cyber threat actor. Currently, Gh0st is being dropped.

Multiple – Malware that currently favors at least two vectors. ZeuS, CoinMiner, and Trickbot are currently utilizing multiple vectors. ZeuS is dropped by other malware, but it is also delivered via malvertisement. CoinMiner utilizes the malspam and dropped vectors. Trickbot is dropped by Emotet and also delivered via malspam.

Malspam – Unsolicited emails, which either direct users to malicious web sites or trick users into downloading or opening malware. Top 10 Malware using this technique include NanoCore, Kovter, Dridex, and Cerber.

Network – Malware introduced through the abuse of legitimate network protocols or tools, such as SMB protocol or remote PowerShell. WannaCry and Brambul use this vector.

Malvertisement – Malware introduced through malicious advertisements. Shlayer, a MacOS trojan, is the first malware since June 2018 to rely on this vector within the Top 10 Malware list.

MS-ISAC – eMail Alerts

Tue 11/12/2019 11:52 AM

MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>

MS-ISAC CYBERSECURITY ADVISORY - Critical Patches Issued for Microsoft Products, November 12, 2019 - PATCH: NOW - TLP: WHITE

To Thomas Duffy

This message was sent with High importance.

Phish Alert + Get mor

[EXTERNAL EMAIL - CAUTION: Do not open unexpected attachments or links.]

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2019-122

DATE(S) ISSUED:
11/12/2019

SUBJECT:
Critical Patches Issued for Microsoft Products, November 12, 2019

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Windows
- Internet Explorer
- Microsoft Edge (EdgeHTML-based)
- ChakraCore
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Exchange Server
- Visual Studio
- Azure Stack

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Fusion Centers

- State and major urban area fusion centers (fusion centers) are owned and operated by state and local entities, and are designated by the governor of their state.
- **Primary Fusion Centers:**
  - information sharing and analysis for an entire state
  - highest priority for the allocation of available federal resources,
- **Recognized Fusion Centers:**
  - information sharing and analysis for a major urban area

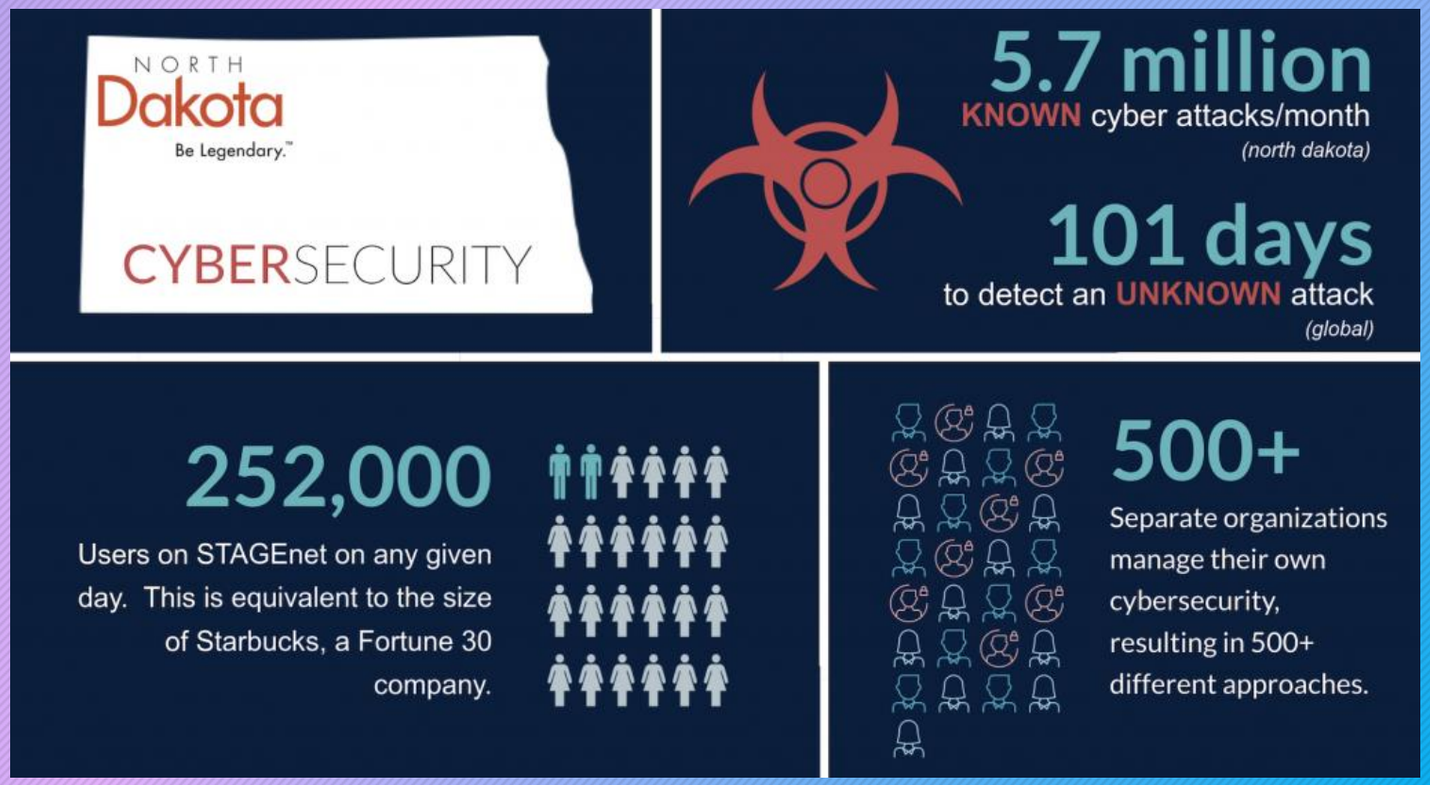
Alaska Information and Analysis Center (Primary)
907-269-8900 / 855-692-5425

North Dakota's IT department takes charge of cybersecurity for the entire state

Cybersecurity unification

- Two-year budget, 2020-21, $174 million
- upgrading voting integrity, public safety and government service interfaces

$16.4 *million*
17 new full-time cybersecurity employees



Alaska Unified Security Operations Center ??

- Department of Administration
  - Office of Information Technology
    - Chief Information Security Officer
- Coalition of State, Borough, City, Tribal

Key Takeaways

Understand

Prepare

Partner

Discussion