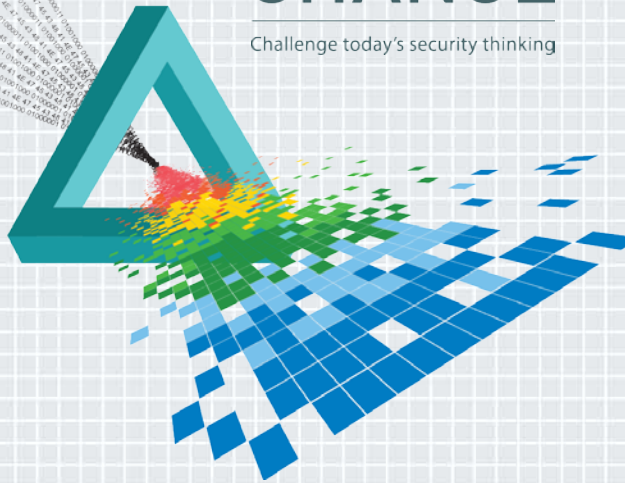
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



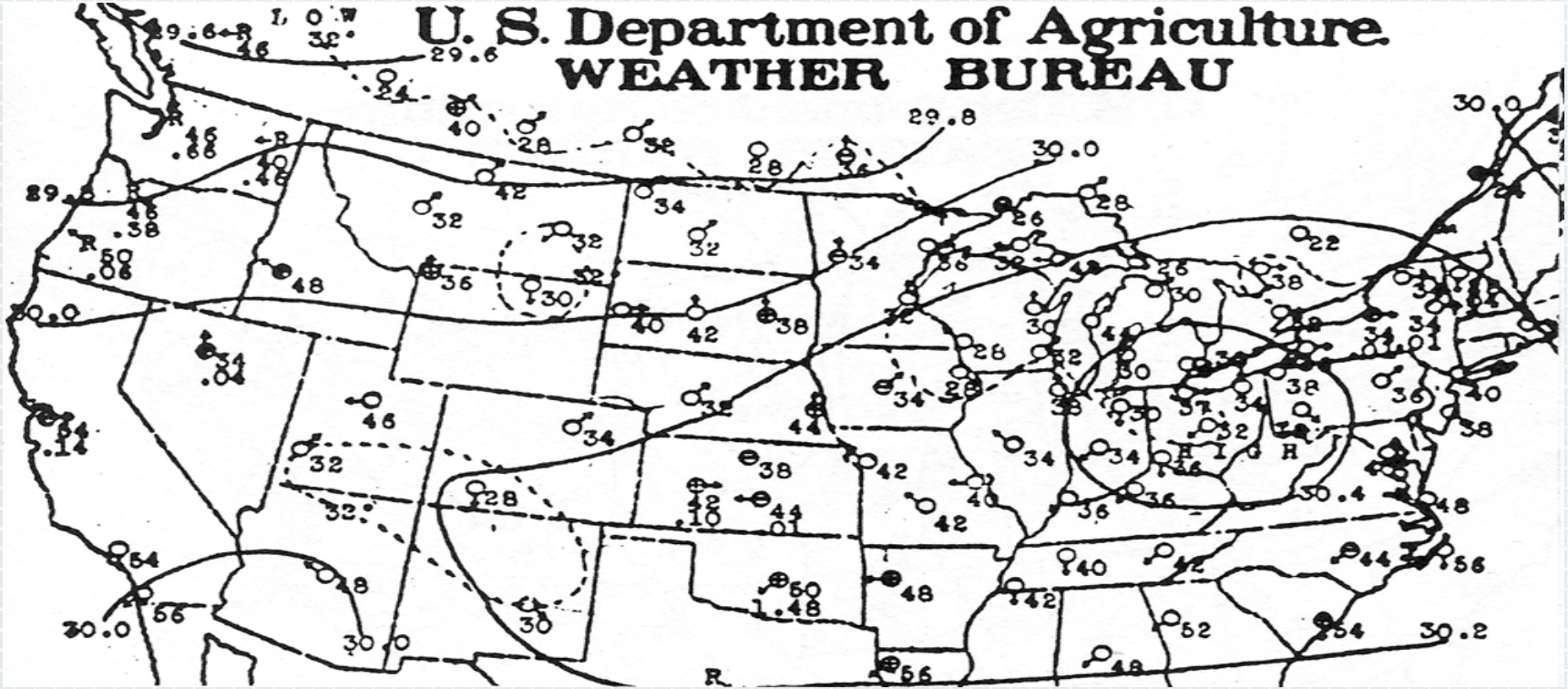
SESSION ID: **HT-W03**

Modern Department of Homeland Security Cyber: Our Vision Forward

Dr. Phyllis Schneck

Deputy Undersecretary for Cybersecurity and Communications
Department of Homeland Security
@Cyber

Industrial Age WxMap



November 10th, 1913

November 13th, 1913

THE WEATHER:—
Tonight, fair, colder:
Moderate west winds.

The Detroit News

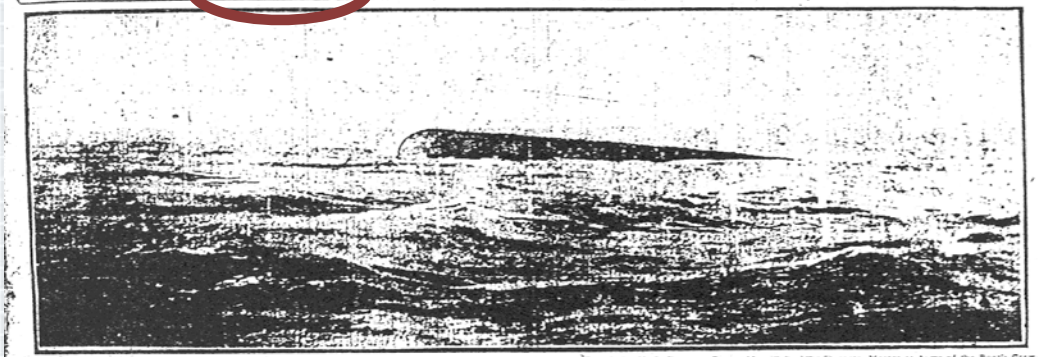
LATEST EDITION

51ST YEAR, NO. 82. DETROIT, MICHIGAN, THURSDAY, NOVEMBER 13, 1913.—TWENTY-FOUR PAGES.

DEATH TOTAL ON LAKES MAY BE 273

WILSON READY TO AID REBELS

GREATEST MYSTERY IN HISTORY OF GREAT LAKES DISASTERS



This Photograph of the Overturned Boat, the Identity of Which Nobody Has Been Able to Learn, Was Taken on Board the U. S. Revenue Cutter Morrill by John Ehrcotta, Master-at-Arms of the Boat's Crew. It Is the Only Photograph Taken to Date of the Strange Wreck.

DISASTER GROWS AS NEW REPORTS COME

DEAD AND MISSING ON GREAT LAKES.

Carruthers	28	Isaac M. Scott	28
Regina	22	Butters	20
McGean	28	Plymouth	7
Wexford	22	Leafield	15
Price	28	Lightship No. 62	6
Argus	26	Nottingham	3
Lafayette	12		
Hydrus	28		
Total			273

Vessel men estimate the financial loss at $3,000,000.

DEATH AND LOSS TOTALS MOUNT; MAY PROVE STORM WORST KNOWN

Mysteries Still Unsolved.

THAT DEPOT LOOP SHOULD BE BUILT

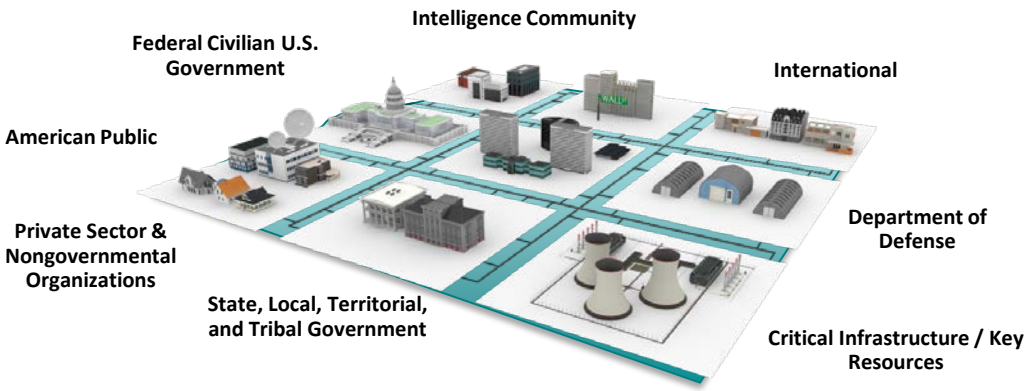
WAITS TILL U.S. ENVOYS QUIT MEXICO

GIVES BLOOD TO BROTHER IN VAIN

SHIP MYSTERY IS NO NEARER A SOLUTION

Need Enhanced and Interoperable Capabilities Across Ecosystem

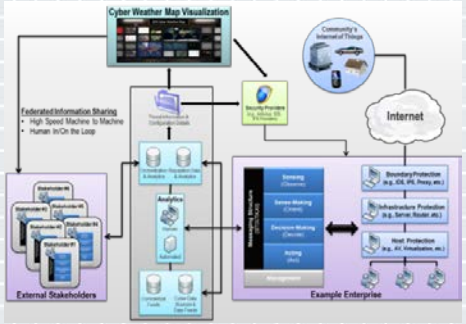
Protecting and enhancing the Nation's cyber and physical critical infrastructure is a ***shared responsibility.***

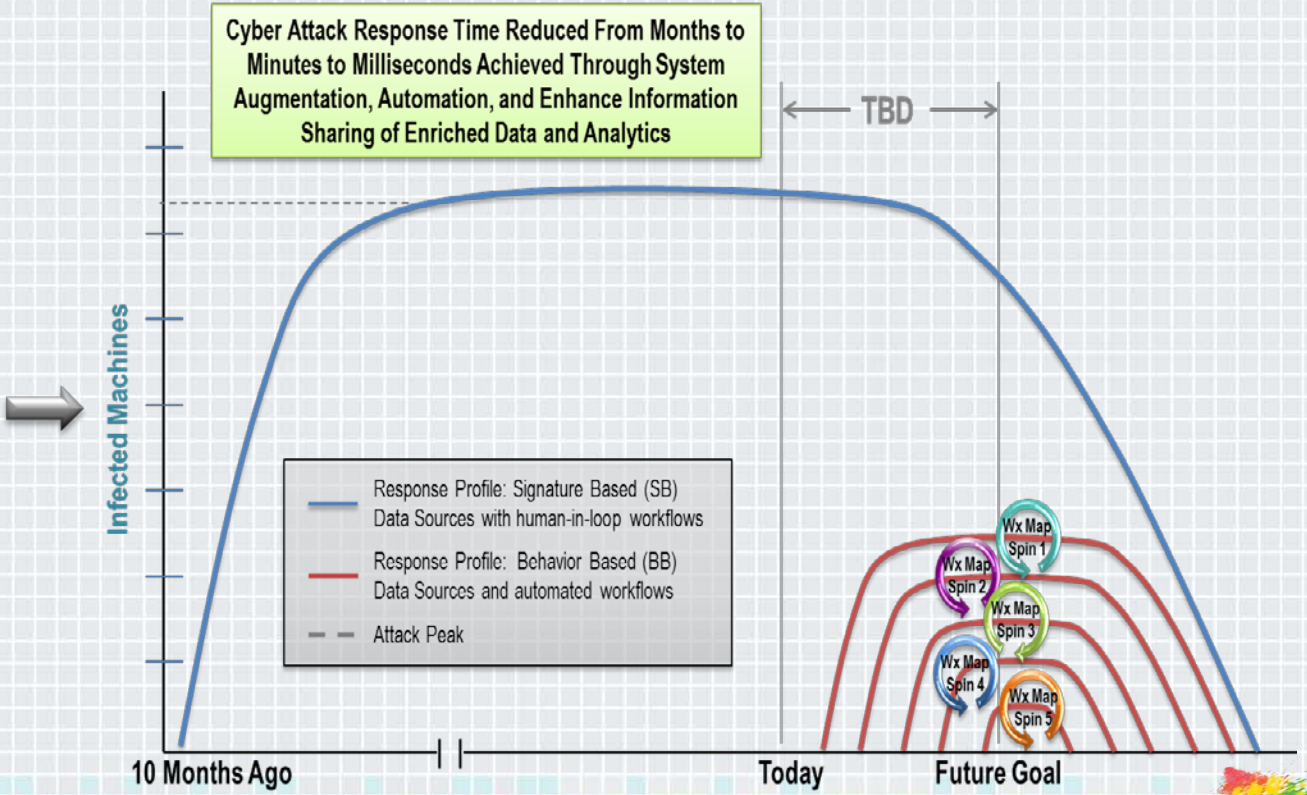


Enterprise Owners and Operators retain primary responsibility, while DHS helps to evolve the Cybersecurity, Communications, and Physical Ecosystem.

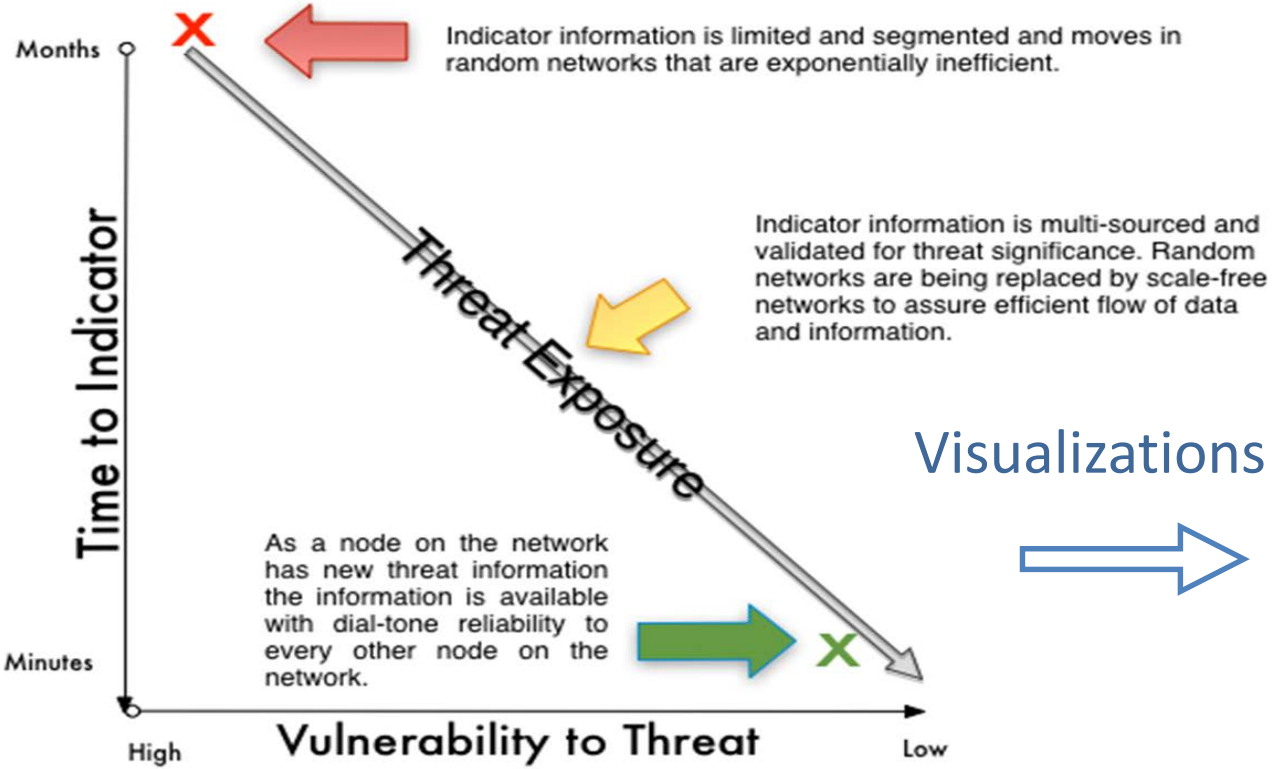
Cyber Attack Response: Months to Milliseconds

Integrated Adaptive Cybersecurity Defense (IACD)





Risk Reduction at the Speed of the Network



Visualizations

What is the DHS Cyber Weather Map?

Cyber Weather Map

An integrating initiative that ***harnesses*** NPPD Programs and Mission Operations to enable:

Tailorable and Protected Information Sharing and Situational Awareness

Providing trusted access, aggregation and analysis across commercial and Government-based sources

Rapid Access to Enriched, Trusted Indicators and Mitigations

Providing high confidence reputation information, behavior-based indicators, and mitigations at cyber relevant speeds

Unity of Effort for Cyber Readiness and Response

Providing coordinated cyber response planning/execution and scalable net-speed cyber defense capabilities

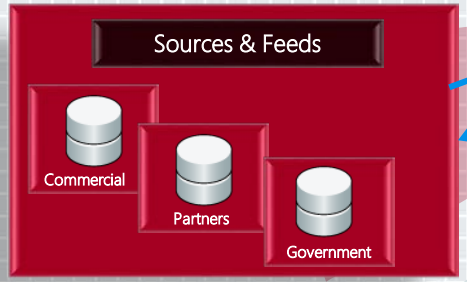
Cyber Weather Map

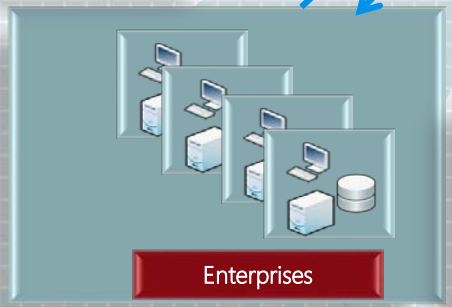
Analysis/Planning/Response

Advanced Analytics

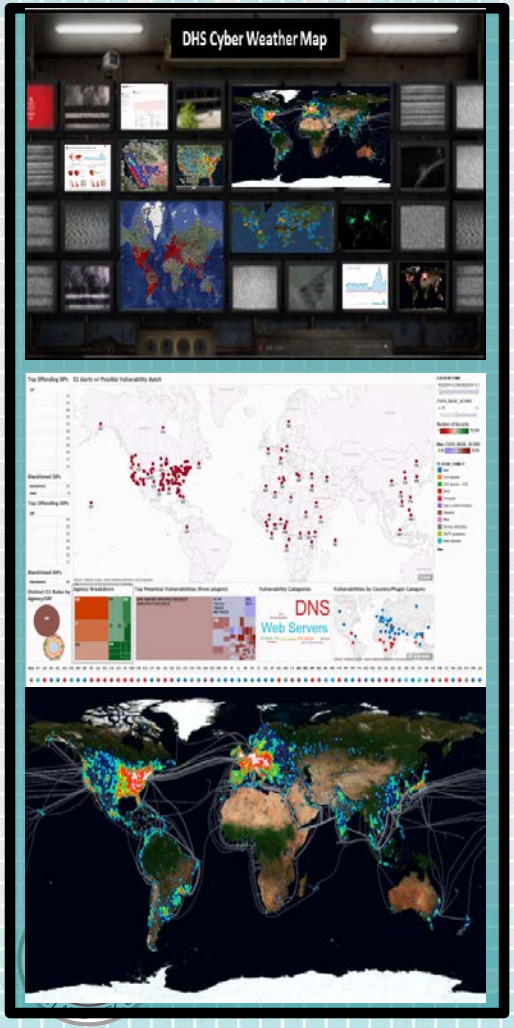
Information Sharing

Data/Sensor Inputs/Indicators





Cyber Weather Map capabilities support and are supported by multiple sources, enterprises, partners

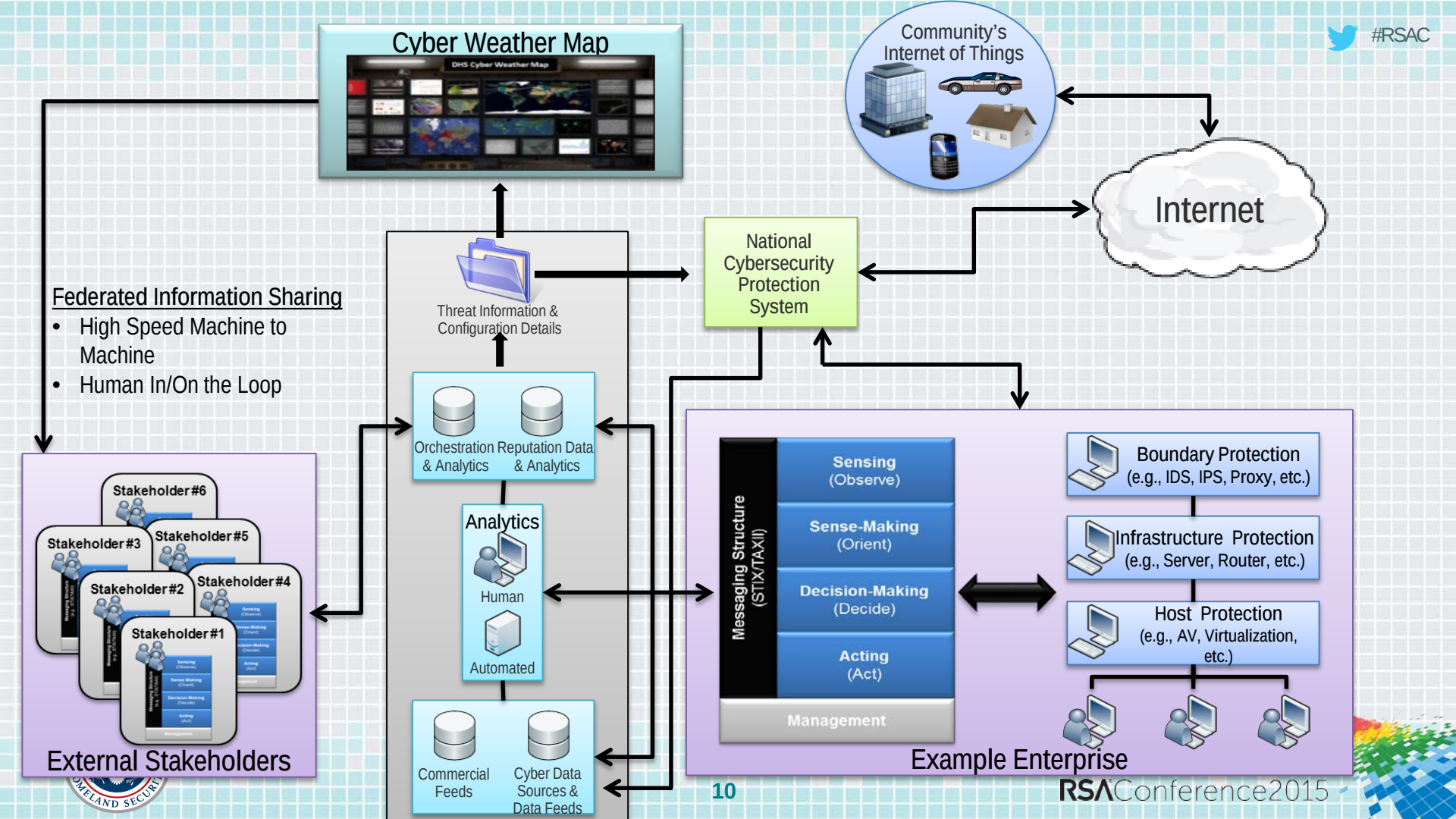


High Speed Cybersecurity Automation

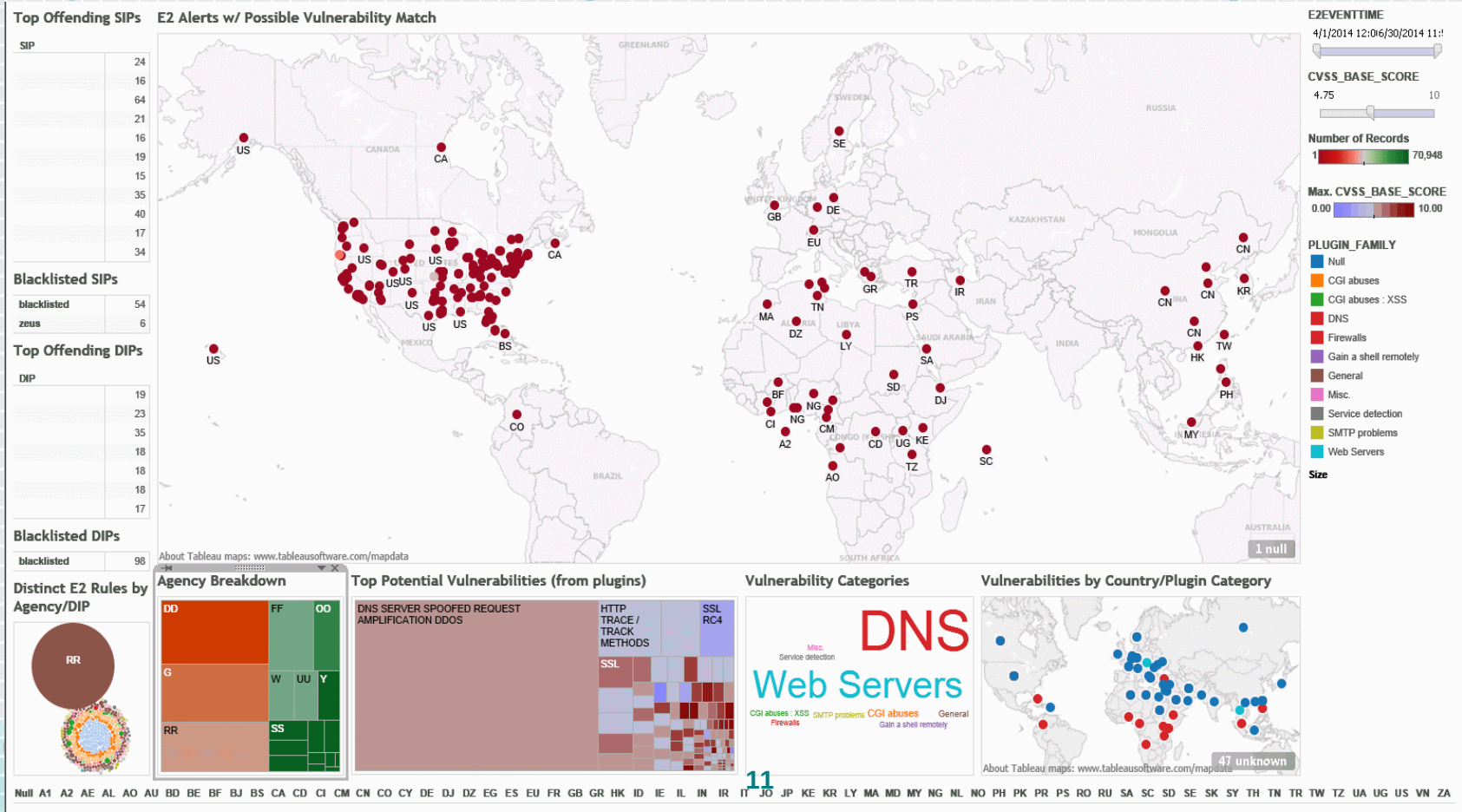
"If You See Something, Say Something™"

Example Questions:

1. Are we under attack?
2. Who is attacking?
3. What are the consequences?
4. What are the next targets?


Cyber Weather Map
DHS Cyber Weather Map
Community's Internet of Things
Internet
National Cybersecurity Protection System
Federated Information Sharing
• High Speed Machine to Machine
• Human In/On the Loop
Threat Information & Configuration Details
Orchestration & Analytics
Reputation Data & Analytics
Analytics
Human
Automated
Commercial Feeds
Cyber Data Sources & Data Feeds
Stakeholder #6
Stakeholder #3
Stakeholder #5
Stakeholder #2
Stakeholder #4
Stakeholder #1
External Stakeholders
Messaging Structure (STIX/TAXII)
Sensing (Observe)
Sense-Making (Orient)
Decision-Making (Decide)
Acting (Act)
Management
Boundary Protection (e.g., IDS, IPS, Proxy, etc.)
Infrastructure Protection (e.g., Server, Router, etc.)
Host Protection (e.g., AV, Virtualization, etc.)
Example Enterprise

Cyber Weather Map Visualization Example



Get More Involved With DHS

- Explore CDM
  - Overview: https://www.us-cert.gov/sites/default/files/cdm_files/CDM_ProgramOverview.pdf
  - Public website: www.dhs.gov/cdm
- Share with the NCCIC
  - Website: https://www.us-cert.gov/nccic

Apply what you have learned today: Get More Involved With DHS

- Learn about how to become a part of the CISCP Program
  - Email: CISCP_Coordination@dhs.gov
  - CISCP Program & Governance questions
- Learn about and leverage STIX/TAXII
  - STIX: http://stix.mitre.org
    - List registration: http://stix.mitre.org/community/registration.html Discussion archives: http://making-security-measurable.1364806.n2.nabble.com/STIX-Discussion-List-f7579090.html
    - Tools: https://github.com/STIXProject
  - TAXII: http://taxi.mitre.org
    - Tools & Scripts: https://github.com/TAXIIProject