Coordinating Attack Response at Internet Scale (CARIS)

Overview and Summary Report
July 2015

Kathleen Moriarty
Security Area Director, IETF
Kathleen.Moriarty.ietf@gmail.com

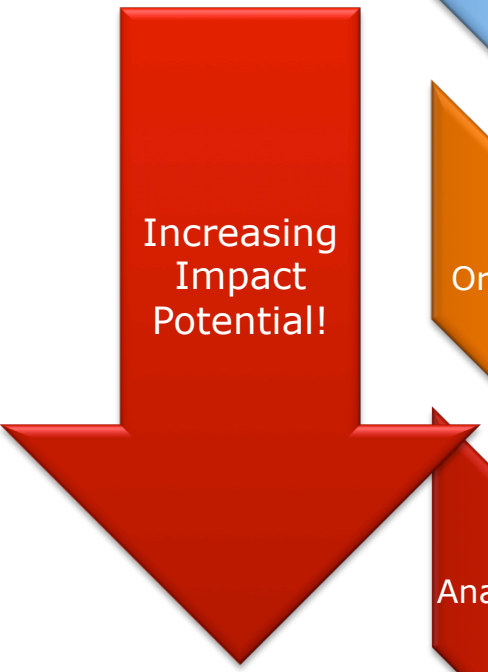
Agenda

- Coordinating Attack Response at Internet Scale (CARIS) Workshop Motivation
- Efficient and Effective Information Exchanges
- Outcomes
- Next Steps

CARIS Workshop

- Bring together diverse groups to better collaborate and scale attack response
  - CSIRTs
  - Operators
  - Researchers
  - Vendors
  - Standards Researchers
- Library of response efforts and how to collaborate with each, Internet Society
  - https://internetsociety2.wufoo.com/reports/caris-workshop-template-submissions/

Who is Sharing Data? What is Useful?



Small & Medium Organizations

- Deploying security technologies with expectation of threat mitigation

Data exchange & actions hidden

Large Organizations

- Deploying security technologies with expectation of threat mitigation
- Participating in multiple sharing groups
- Receiving multiple threat intelligence feeds

Data exchange & actions: Hidden & Exposed

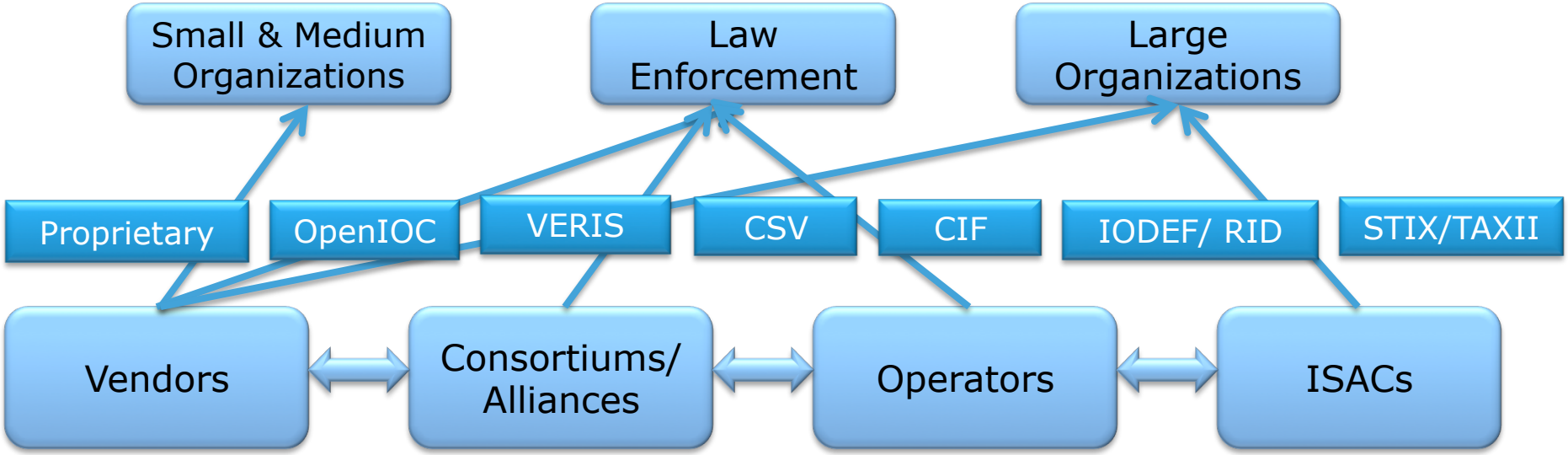
Analysis Center

- Analysis for industry focused or other sharing groups
- National CSIRTs providing information to government, critical infrastructure, etc.
- Internet Service Providers performing analysis, eliminating/mitigating threats
- Problem specific analysis groups targeting focused threats (analysis & mitigation)

Analysis & actions: Data exposed & use case/user group specific

Use Case Driven Adoption

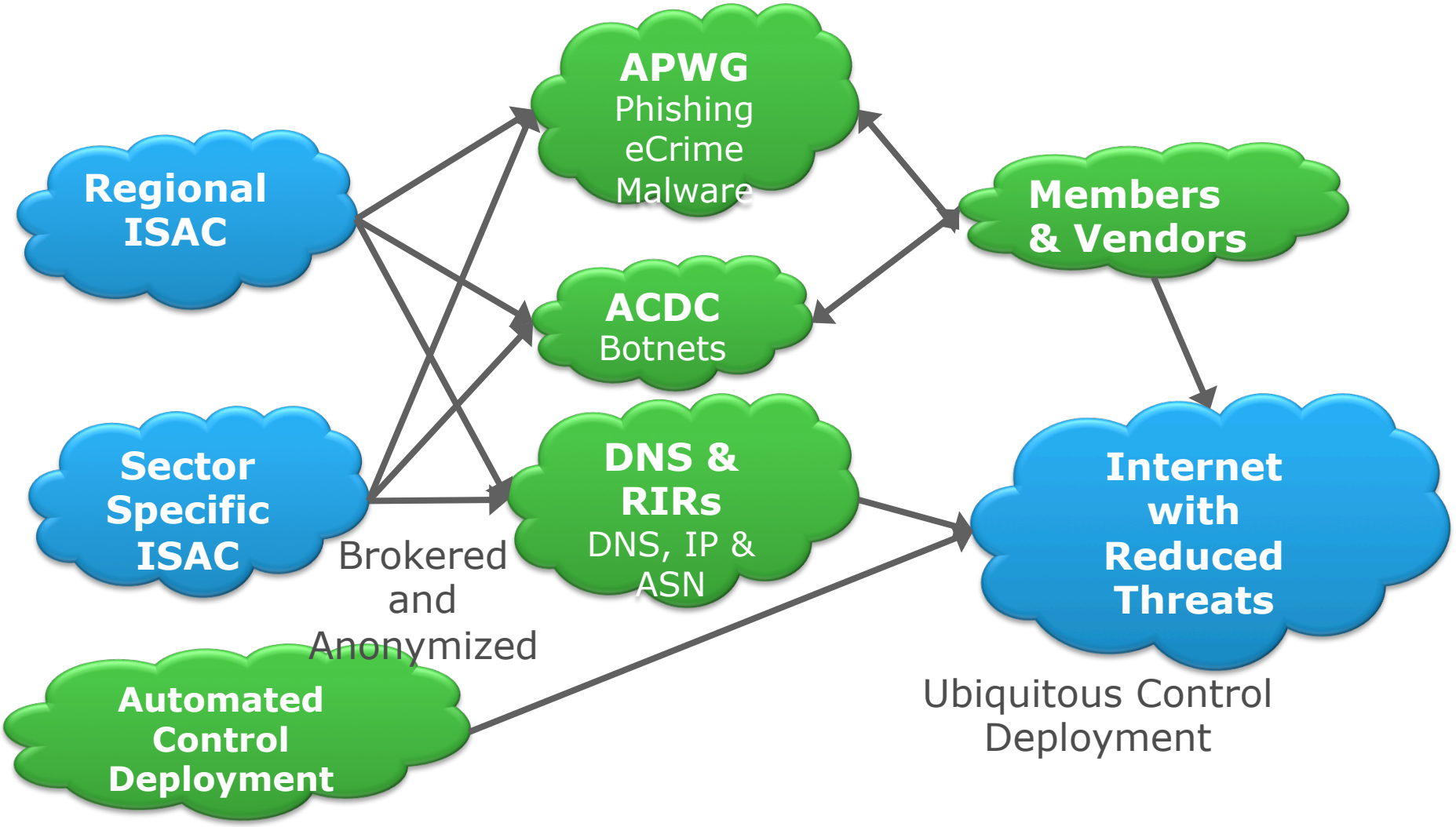
One Size Does Not Fit All



- Shared threat intelligence must be:
  - **Directed**: Intelligence received must be relevant to the organization
  - **Actionable**: Intelligence must identify an immediate and active security response that mitigates the risk
  - **Automated**: Remediation based on intelligence must NOT impact the user experience

Potential Collaborations

Regional & Sector Specific ISACS with Operational Communities



CARIS Workshop Discussions

- Information Sharing groups – Template submissions
  - Describe your use case?
  - Where they are focusing?
  - How can others engage with them?
  - Who participates?
- DDoS and Botnet Talk & Panel
  - Scaling Responses to DDoS and Botnets Effectively and Safely
- Infrastructure: DNS & RIRs
  - What part do they play in incident response
  - Available resources
- Trust, Privacy & Data Markings
- Internet Architecture: How can we help?

Identified Next Steps

Sampling of possible next steps, report may contain additional recommendations

- Education and outreach on Best Practices
  - Simple measures like BCP 38 (ingress/egress filtering) are not widely deployed and could reduce problems
  - Identify additional best practices and determine if updates are needed
- Assist RIRs with improved tools to better scale access to their public resources to assist operators and CSIRTs
- Protocol options to exchange formatted data
  - Too many exist
  - Not enough published information comparing options
  - May require problem specific solutions, such as the exchange of telemetry data for DDoS in DOTS
  - Protocol reviewers needed in SACM and MILE
- Interest expressed for future meetings, organized by neutral organization (ISOC, IAB, etc.)

Program Committee Members

A BIG thank you to all the program committee members and sponsors!

- Program Committee:
  - Matthew Ford, Internet Society, UK
  - Ted Hardie, Google
  - Joe Hildebrand, Cisco, USA
  - Eliot Lear, Cisco, Switzerland
  - Kathleen M. Moriarty, EMC Corporation, USA
  - Andrew Sullivan, Dyn
  - Brian Trammell, ETH Zurich, Switzerland
- Sponsors:
  - Forum for Incident Response and Security Teams (FIRST)
  - The Internet Society
  - EMC Corporation

Thank you!