

# Making the Most of A Lot [of Data]: Netflow in US-CERT Operations

14 January 2015



**Homeland  
Security**

National Cybersecurity and  
Communications Integration Center

# “To-Do” List

- Who’s Einstein?
- A Lot of Data: Challenges of Scale and Diversity
- The Daily Grind
- The Art of the Possible
- Where We Go From Here



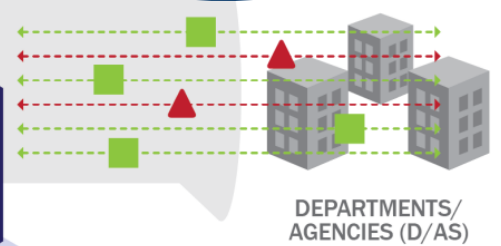
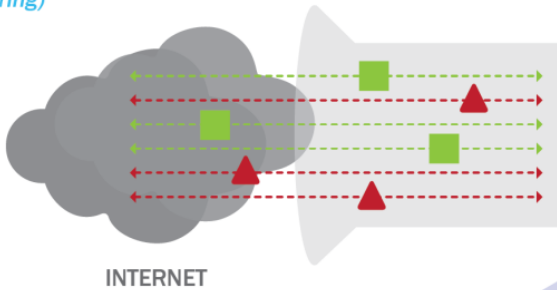
# EINSTEIN OVERVIEW



Hello – My Name Is...

**THREAT INTELLIGENCE**  
(Commercial Threat Feeds, Open Source, Govt Sources, Private Sector Sharing)

**VETTING**  
(Technical/Accuracy/Value, Adhere to DHS Privacy Criteria)



Threat intelligence inputs are carefully vetted then processed through Einstein against incoming network traffic to **PROTECT**, **DETECT**, and **ANALYZE** cybersecurity threats and suspicious activity. The Einstein capabilities allows analysts to detect & diagnose current threat activity, perform retrospective analysis on past activity, and mitigate current and future threat activity.



**OUTPUTS**  
(Situational Awareness, Report/Notify D/As, IRT Support, General Monitoring)

# A \*Lot\* of Data: The Quantifiable

- Scale:
  - ~17B flows/day
  - decent chunk of storage
- Diversity:
  - 300+ sensors
  - 100+ organizations
  - ~39M IP addresses monitored
    - ~9M observed/day
    - ~45M IP addresses observed/day
    - ~3B IP addresses observed all-time



# A Lot of \*Different\* Data: The Unquantifiable



## Wide Range of Missions

Citizen Services, to Tourism, to Science and so much more.



## Geographic Dispersion

National & International... every time zone.



## Both a Large Producer & Large Consumer



## Varied Usage & Security Filtering Policies



# The Ever-evolving Network Landscape

- Thorns in the netflow analyst's side, some old, some more recent:
  - NATs/proxies
  - Cloud services / shared hosting
  - Protocol convergence – Everything is HTTP(S)
  - IPv6 – a briefer's nightmare
- Encryption? No content, no problem - right?
  - Depends on implementation and sensor placement
  - The NAT/proxy problem all over again



# Yet Against All the Odds....

- Netflow remains an integral tool

## Common US-CERT Use Cases



Augments signature-based alert data (detailed timestamps, pattern of activity vs. one-off, indicators of attack success)



Retrospective analysis – particularly in support of deployed incident response teams



Statistical/behavioral analysis still quite valid for certain types of threats (i.e. volume-based)



Assess viability of new threat indicators

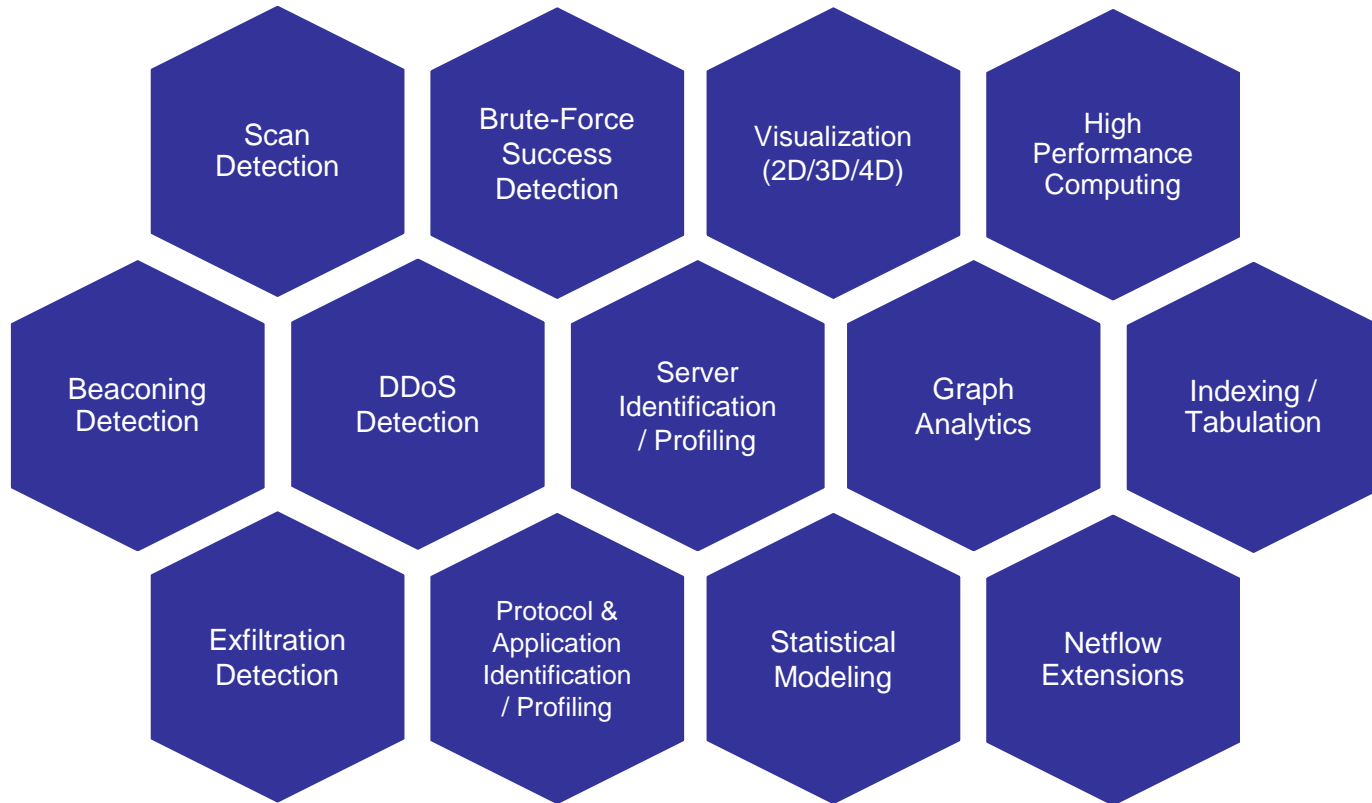


Assess exposure / attack surface for new vulnerabilities



# The Art of the Possible

- Our community has a wide body of fantastic research.
- Effective operational implementations are hard...but maybe we can help.





# Where We Go From Here

- Questions/Discussion
- Help Us, Help You, Help Us

[networkanalysis@us-cert.gov](mailto:networkanalysis@us-cert.gov)

Chad Hein

[chad@phiatech.com](mailto:chad@phiatech.com)



Homeland  
Security

National Cybersecurity and  
Communications Integration Center