IBM Cognitive Cyber Defense

IARPA CAUSE

IBM'S MACHINE LEARNING CYBER SECURITY SOLUTION

21 January 2015

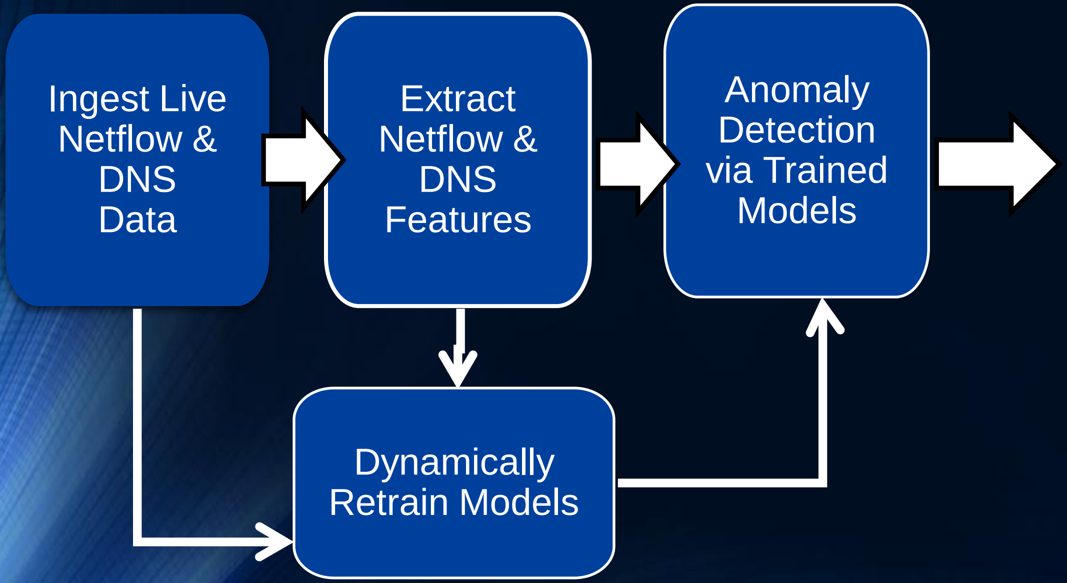
Greg Porpora
IBM Federal Chief Engineer Cognitive Computing & Analytics

IBM's Cognitive Cyber Defense
Advanced Persistent Threat (APT) Network Detector

- Machine Learning Based APT Detector comprised of a family of Supervised and Unsupervised models
  - Analyzes Net Flow and/or DNS data in real-time
  - Can scale to 32TB per day
  - Advanced reporting capabilities
  - Botnet topology reconstruction via I2
  - Cyber Command Center View
  - Deep Forensic drill down
- Cots Based Technology : SPSS, Infosphere Streams, Cognos BI
- Open API's with support to Hadoop clouds, Qradar, SIEM's, other data repositories

Netflow & DNS -based Advanced Persistent Threat Anomaly Detection

- **Detect anomalous behavior as it appears**
- **Real-time detection in seconds of unknown attacks**
- **Can easily scale to 32TB per day ingest**
- **Models dynamically adapt to changing signatures**



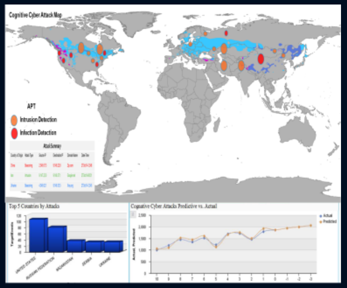
Ingest Live Netflow & DNS Data

Extract Netflow & DNS Features

Anomaly Detection via Trained Models

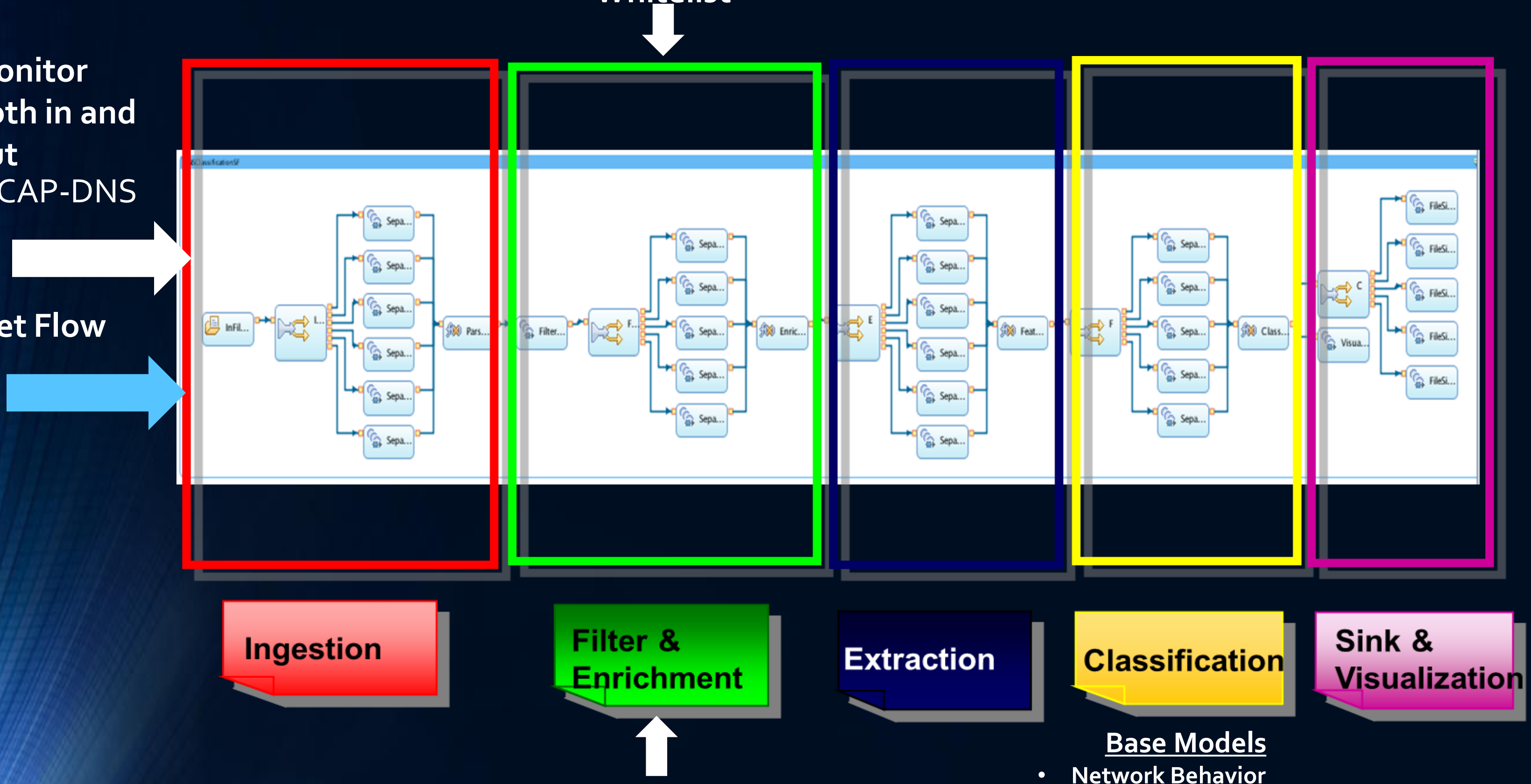
Dynamically Retrain Models

Visualization



Real Time Advanced Persistent Threat Detection
Botnet Fast Flux Aggregate Activity
Botnet Fast Flux Aggregate Country View
Botnet Fast Flux Aggregate Domain Specific View
Botnet Fast Flux Aggregate Target Specific View

Cognitive Cyber Defense basic real-time Cyber analysis workflow inside Infosphere Streams



Blacklist
&
Whitelist

Monitor both in and out PCAP-DNS

Net Flow

Ingestion

Filter & Enrichment

Extraction

Classification

Sink & Visualization

WHOIS or Maxmind

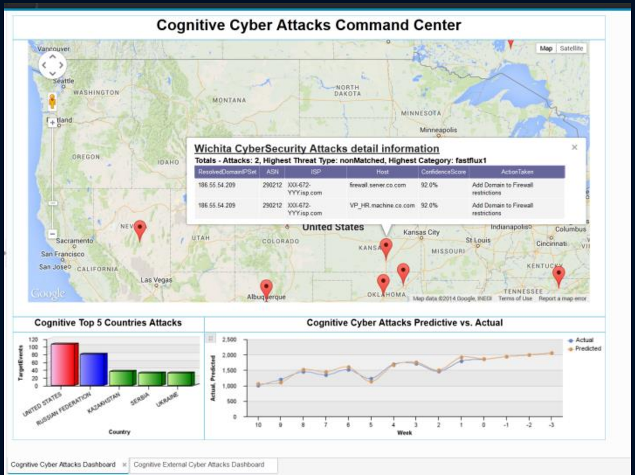
Base Models

- Network Behavior Modeling
- Fast Fluxing
- DNS Amplification Attacks
- DNS Poisoning
- DNS Tunneling
- Net Flow Behavior Modeling

Beaconing-Exfiltration tests

- Compare detected Fast Flux DNS and associated IP addresses performing Intrusion to outbound DNS-IP traffic for matches
- Match real-time behavior-signature to historically derived and dynamically updated

CCD – Visualizing Threats



Wichita CyberSecurity Attacks detail information

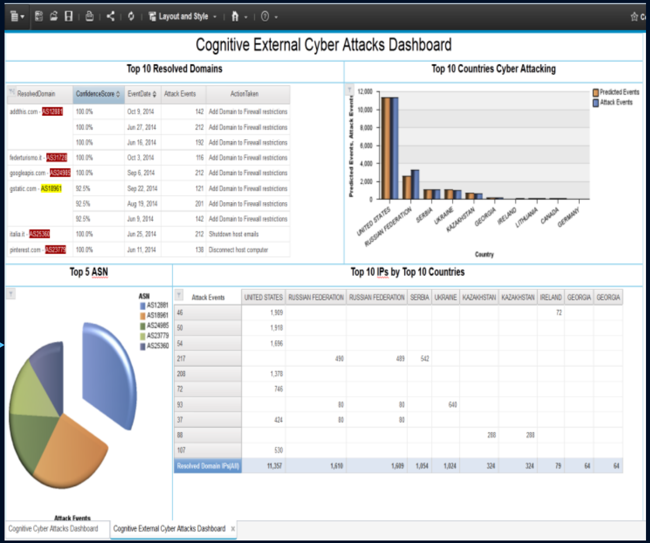
Totals - Attacks: 2, Highest Threat Type: nonMatched, Highest Category: fastflux1

ResolvedDomainIPSet	ASN	ISP	Host	ConfidenceScore	ActionTaken
186.55.54.209	290212	XXX-672-YYY.isp.com	firewall.server.co.com	92.0%	Add Domain to Firewall restrictions
186.55.54.209	290212	XXX-672-YYY.isp.com	VP_HR.machine.co.com	92.0%	Add Domain to Firewall restrictions

(Cognos)

← APT Detection

Forensic Analysis →



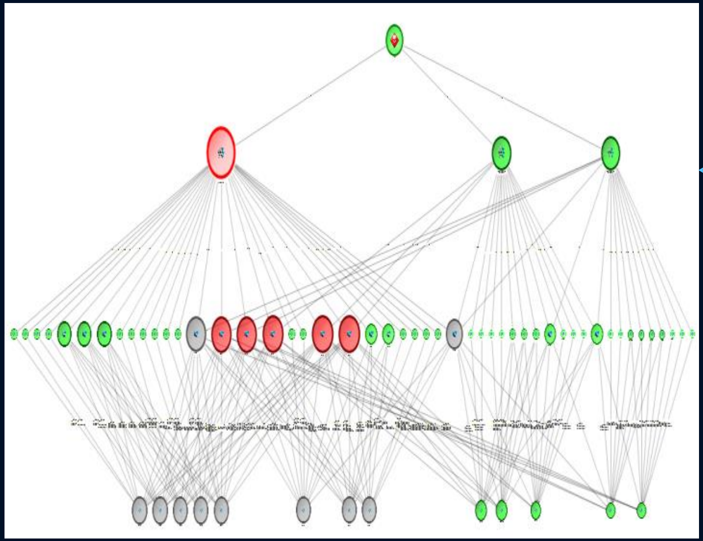
Cognitive External Cyber Attacks Dashboard

Top 10 Resolved Domains

ResolvedDomain	ConfidenceScore	EventDate	Attack Events	ActionTaken
addthis.com - AS12881	100.0%	Oct 9, 2014	142	Add Domain to Firewall restrictions
	100.0%	Jun 27, 2014	212	Add Domain to Firewall restrictions
	100.0%	Jun 16, 2014	192	Add Domain to Firewall restrictions
federturismo.it - AS31728	100.0%	Oct 3, 2014	116	Add Domain to Firewall restrictions
googleapis.com - AS24985	100.0%	Sep 6, 2014	212	Add Domain to Firewall restrictions
gstatic.com - AS18961	92.5%	Sep 22, 2014	121	Add Domain to Firewall restrictions
	92.5%	Aug 19, 2014	201	Add Domain to Firewall restrictions
	92.5%	Jun 9, 2014	142	Add Domain to Firewall restrictions
italia.it - AS25360	100.0%	Jun 25, 2014	212	Shutdown host emails
pinterest.com - AS23779	100.0%	Jun 11, 2014	138	Disconnect host computer

Top 10 IPs by Top 10 Countries

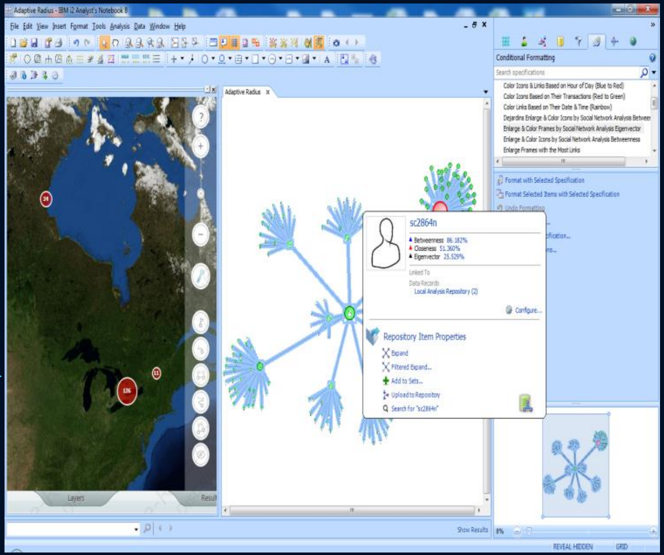
Attack Events	UNITED STATES	RUSSIAN FEDERATION	RUSSIAN FEDERATION	SERBIA	UKRAINE	KAZAKHSTAN	KAZAKHSTAN	IRELAND	GEORGIA	GEORGIA
46	1,909							72		
50	1,918									
54	1,696									
217		490	489	542						
208	1,378									
72	746									
93		80	80		640					
37	424	80	80							
88						288	288			
107	530									
Resolved Domain IPs(All)	11,357	1,610	1,609	1,054	1,024	324	324	79	64	64



(i2)

← Botnet Topology and Attack Reconstruction

Adaptive Profiling →



Conditional Formatting

Search specifications

Color Icons & Links Based on Hour of Day (Blue to Red)
Color Icons Based on Their Transactions (Red to Green)
Color Links Based on Their Date & Time (Rainbow)
Dejardins Enlarge & Color Icons by Social Network Analysis Betweer
Enlarge & Color Frames by Social Network Analysis Eigenvector
Enlarge & Color Icons by Social Network Analysis Betweenness
Enlarge Frames with the Most Links

Format with Selected Specification
Format Selected Items with Selected Specification
Undo Formatting

sc2864n

Betweenness 86.182%
Closeness 51.360%
Eigenvector 25.529%

Linked To
Data Records
Local Analysis Repository (2)

Configure...

Repository Item Properties

Expand
Filtered Expand...
Add to Sets...
Upload to Repository
Search for "sc2864n"