

x January 2018

# FloCon 2018

Tucson AZ

Analysis of DNS Traffic on the Network EDGE, and In Motion.

Fred Stringer

# Key Messages

---

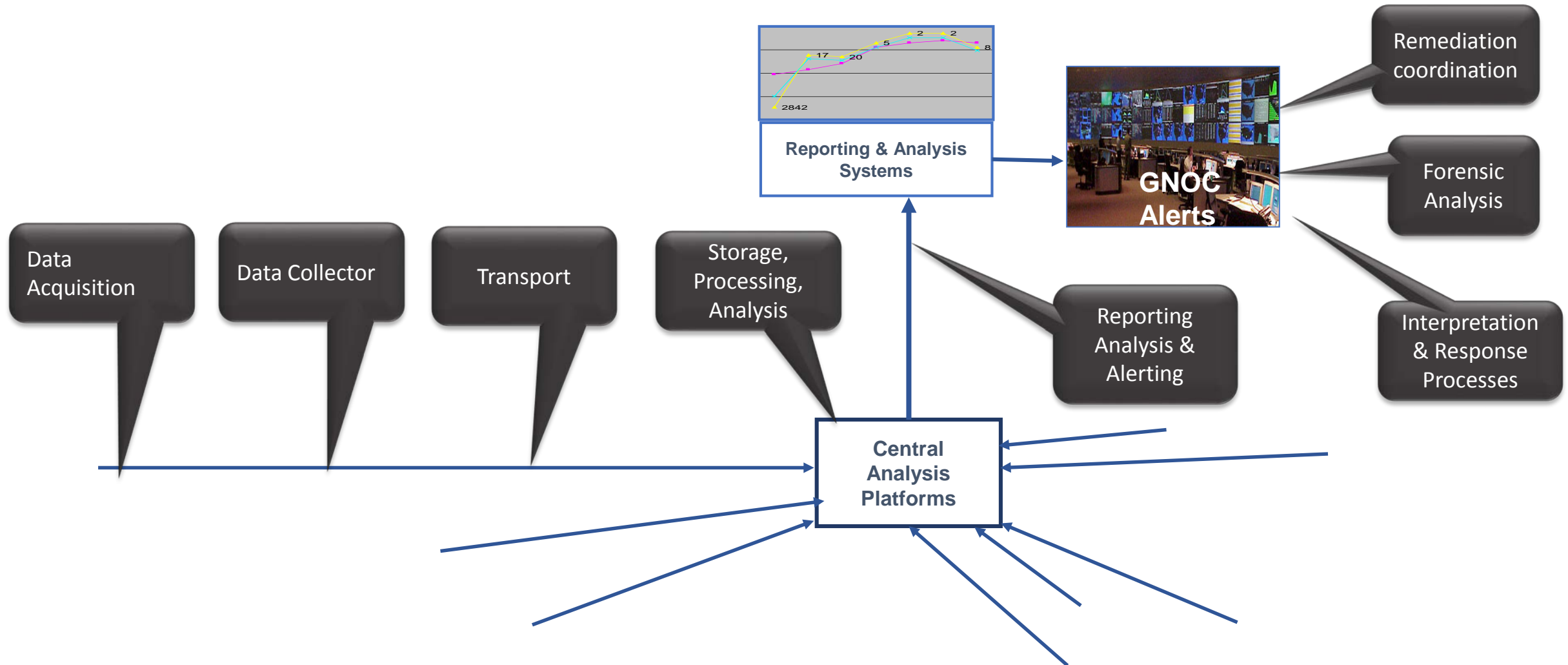
- **Distributed Analysis (at the collection points) enables scale, flexibility and timely indicators.**
- **Streaming analysis enables near real time detection from multiple algorithms with one packet capture and parsing.**
- **Machine learning algorithms with data in motion are accurate and effective.**
  - **More accuracy is achieved with some analysis work, managing block/ignore lists.**
- **COTS commodity hardware is capable of handling respectable volume of traffic ~4Gb/s**

# Two More Observations

---

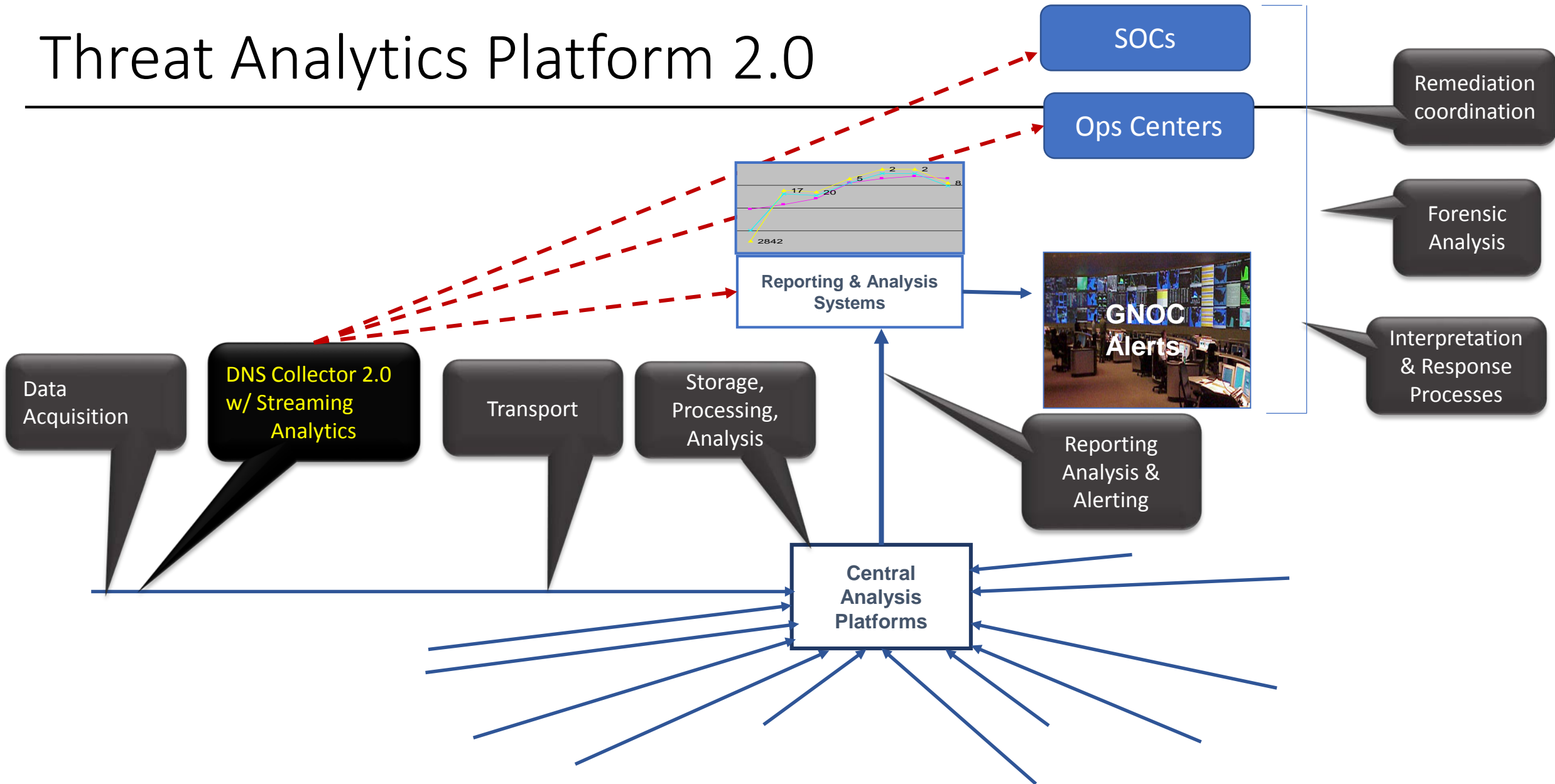
- **Analysis of DNS activity provides insights into security relevant activity that you may not have anticipated.**
- **Traffic analysis provides indicators not seen anywhere else.**
  - **This is Flocon , you all knew that.**

# Threat Analytics Platform 1.5



Source: AT&T Cyber Security Strategy presentation

# Threat Analytics Platform 2.0



Source: AT&T Cyber Security Strategy presentation

# Valuable Security Analysis of DNS Activity 1/3

---

- **Tunneling and other non-DNS over port 53**
  - Detect compromised hosts potentially exfiltrating data.
- **DGA Detection**
  - Identify hosts with indications they are participating in a Botnet
- **Squatting Detection**
  - Identify domains which are impersonating legitimate domains.  
Often used in phishing attacks.
- **Outlier Detection and Volumetric Anomaly Detection.**
  - Indicates a pattern change. Typically prompts additional automated correlation and can reinforce (add confidence level) another indicator.

# Valuable Security Analysis of DNS Activity 2/3

---

- **DrDos – Distributed Reflective Denial of Service**
  - Identify hosts being DDoS attacked, typically Identifies a spoofed address – entry of which is often traced to misconfiguration.
  - Detect of open resolvers.
- **“Dark DNS” - rogue DNS infrastructure**
  - DNS changer and more.
  - Detection of DNS infrastructure outside of the Internet hierarchy typically used for control of malicious activities.
  - Indicates hosts communicating have been potentially compromised

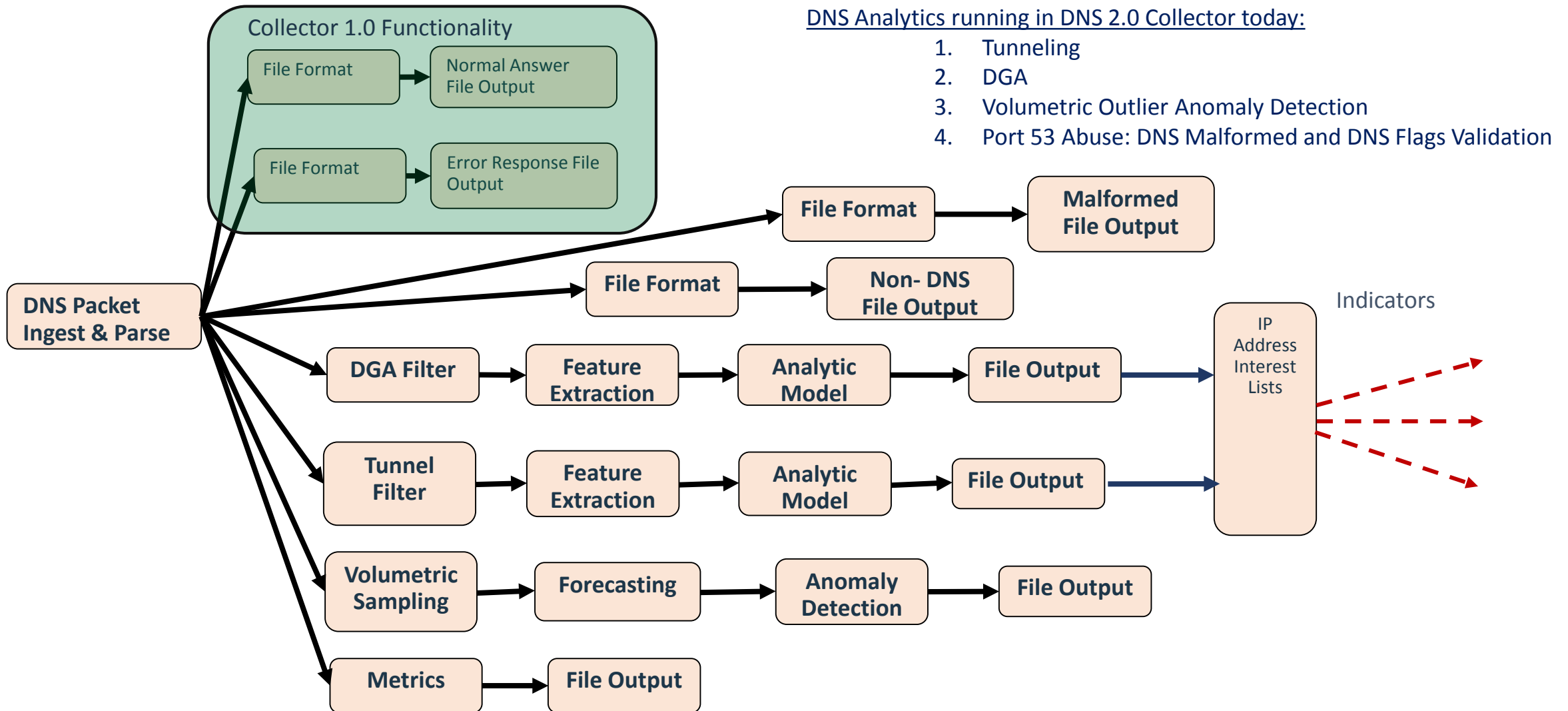
# Valuable Security Analysis of DNS Activity 2/3

---

- **DNS NXDOMAIN and Subdomain exhaust**
  - DoS attack of the DNS impairing service to all users.
  - DNS clients often spoofed and/or compromised host.
- **Newly Observed Domains (NOD)**
  - Useful indicator to correlate with other indicators.
  - Can give NOD a low reputation score initially
  - If today's NOD was and DGA NXDOMAIN yesterday it is strong indication of roving C2 of a DGA Botnet.



# DNS Collector 2.0 - Probe / Collector / Analyzer



# Take-Aways

---

- **Distributed Analysis (at the collection points) enables scale, flexibility and timely indicators.**
- **Real time streaming analysis on the network edge enables detecting multiple indicators simultaneously**
  - **Correlating indicators can strengthen the confidence level.**
- **Machine learning algorithms not just for data at rest**
- **COTS commodity hardware is capable of handling respectable volume of traffic ~4Gb/s**
- **DNS Collector 2.0 can run as NFV in a VM at lower DNS traffic volumes.**
- **Analysis of traffic is always interesting, often revealing and effective means of detecting Threat Indicators.**

# AT&T ThreatTraq

source: <http://techchannel.att.com/threattraq>

## Weekly Cyber Threat Report

File Edit View History Bookmarks Tools Help

AT&T ThreatTraq

techchannel.att.com/threattraq/#

AT&T threat traq

Episodes

AT&T Malware and Network Security Gurus gather weekly to give you the information you need to know about the latest security news and trends.

Watch the latest episode

Episodes

Enter keyword...

<b>12/01/2017</b> <b>'Tis the Season: Necurs and Scarab, Exim, Firefox and Breached Sites</b> Episode #275 and Internet Weather. Scarab Ransomware, Unix mailer Exim affected by RCE, Dns Vulnerabilities, Firefox flag breached sites	<b>11/22/2017</b> <b>Security on the Agenda: Poison Searches, SowBug, Blocking Chrome Redirects</b> Episode #274 - Hackers Poison Google Search, Newly Recovered 'SowBug', Chrome Will Stop Sketchy Sites From Bouncing You To Ads	<b>11/16/2017</b> <b>Fascinating Space: AVGater, PowerShell, Magniber</b> Episode #273 AVGater, Keep an Eye on Your Root Certificates, Magniber Ransomware Wants to Infect Only the Right People	<b>11/06/2017</b> <b>An Evolving Story: CryptoShuffler, GIBON</b> Episode #272 Cryptocurrency Wallets Hacked by 'CryptoShuffler' Trojan, GIBON Ransomware Being Distributed by Malipam
<b>11/02/2017</b> <b>Basic Precautions: BadRabbit, Ransomware Economy, KRACK</b> Episode #271 BadRabbit Technical Analysis, Ransomware Economy, Key Reinstallation Attacks	<b>10/26/2017</b> <b>A Look at the Future: IoTreaper, Stealing SSH, Autonomous Apps</b> Episode #270 - IoT Botnet Threats to Take Over Internet, Scanning for SSH Keys on Websites, Autonomous Protection of Applications	<b>10/18/2017</b> <b>Good to Share: Macroless Malware, Mac Scams, DDoS Train Attacks</b> Episode #269 - Macroless Malware: 'A New Technique with Old Technology', Mac Scams, DDoS Attacks on Sweden - Transport Agencies Delay Train Service	<b>10/12/2017</b> <b>Again Worrisome: DnsMasq Bug, Skimmer Scanners, FormBook</b> Episode #268 - DnsMasq Critical Bug, App Detects Skimmer Scanners at Gas Pumps, FormBook Malware Targets Victims Through Email Campaigns and Internet Weather

Subscribe:

ATT-ThreatTraq-Distri... x +

techchannel.att.com/threattraq/#/video/ATT-ThreatTraq-Distributed-Guessing-Attack

AT&T threat traq

Episodes About Contact

close X

AT&T threat traq

Tis the Season: Necurs and Scarab, Exim, Firefox and Breached Sites