x January 2018

FloCon 2018

Tucson AZ

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

Fred Stringer

Key Messages

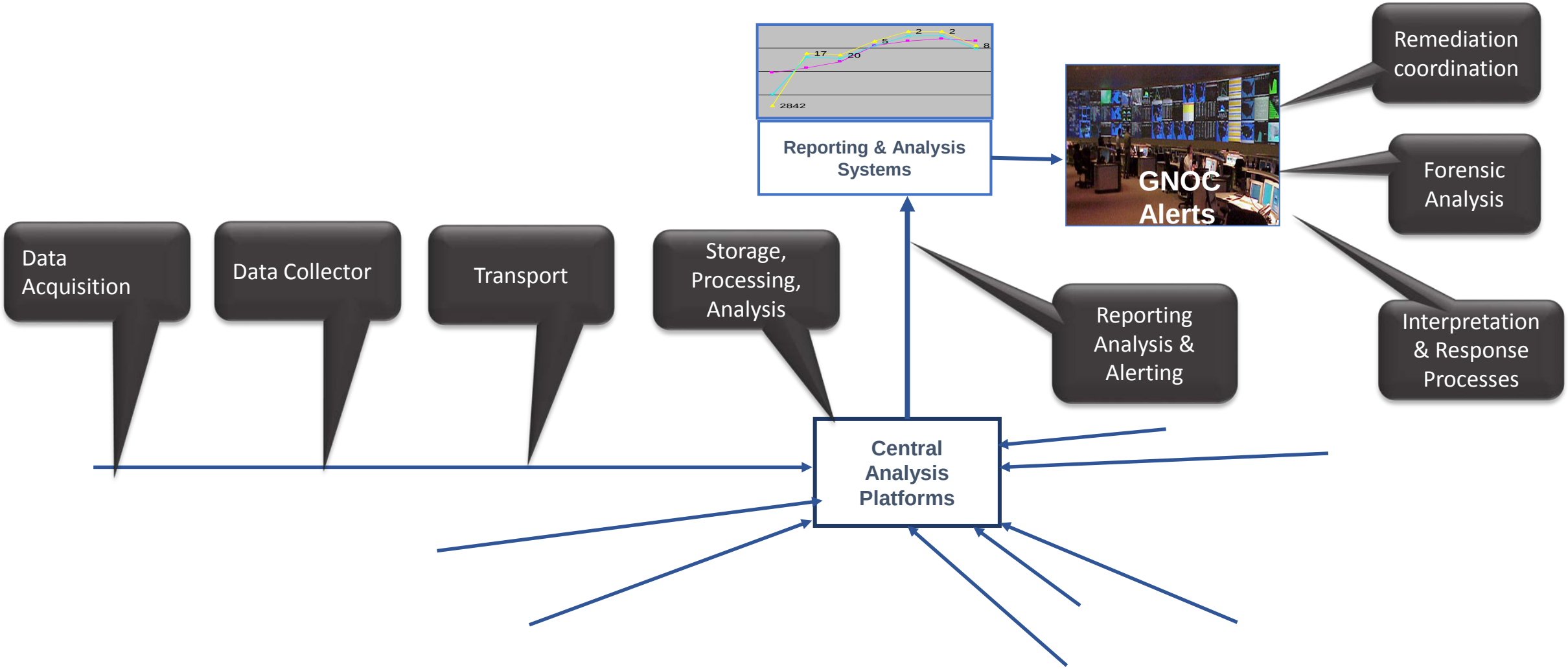
- **Distributed Analysis (at the collection points) enables scale, flexibility and timely indicators.**
- **Streaming analysis enables near real time detection from multiple algorithms with one packet capture and parsing.**
- **Machine learning algorithms with data in motion are accurate and effective.**
  - **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.**

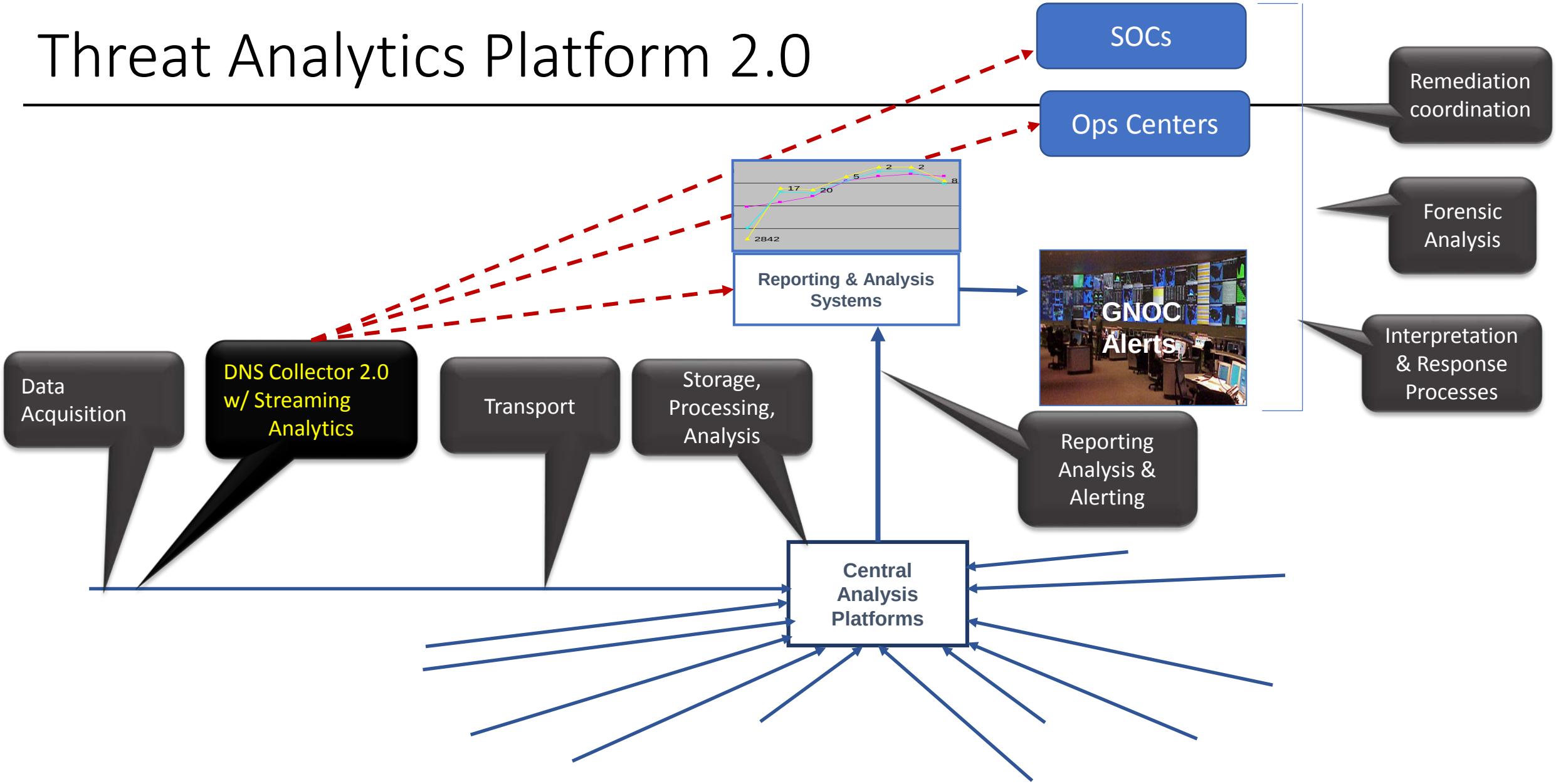
- **Traffic analysis provides indicators not seen anywhere else.**
  - **This is Flocon , you all knew that.**

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.

Source: AT&T DNS Collector 2.0 Feature Description

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

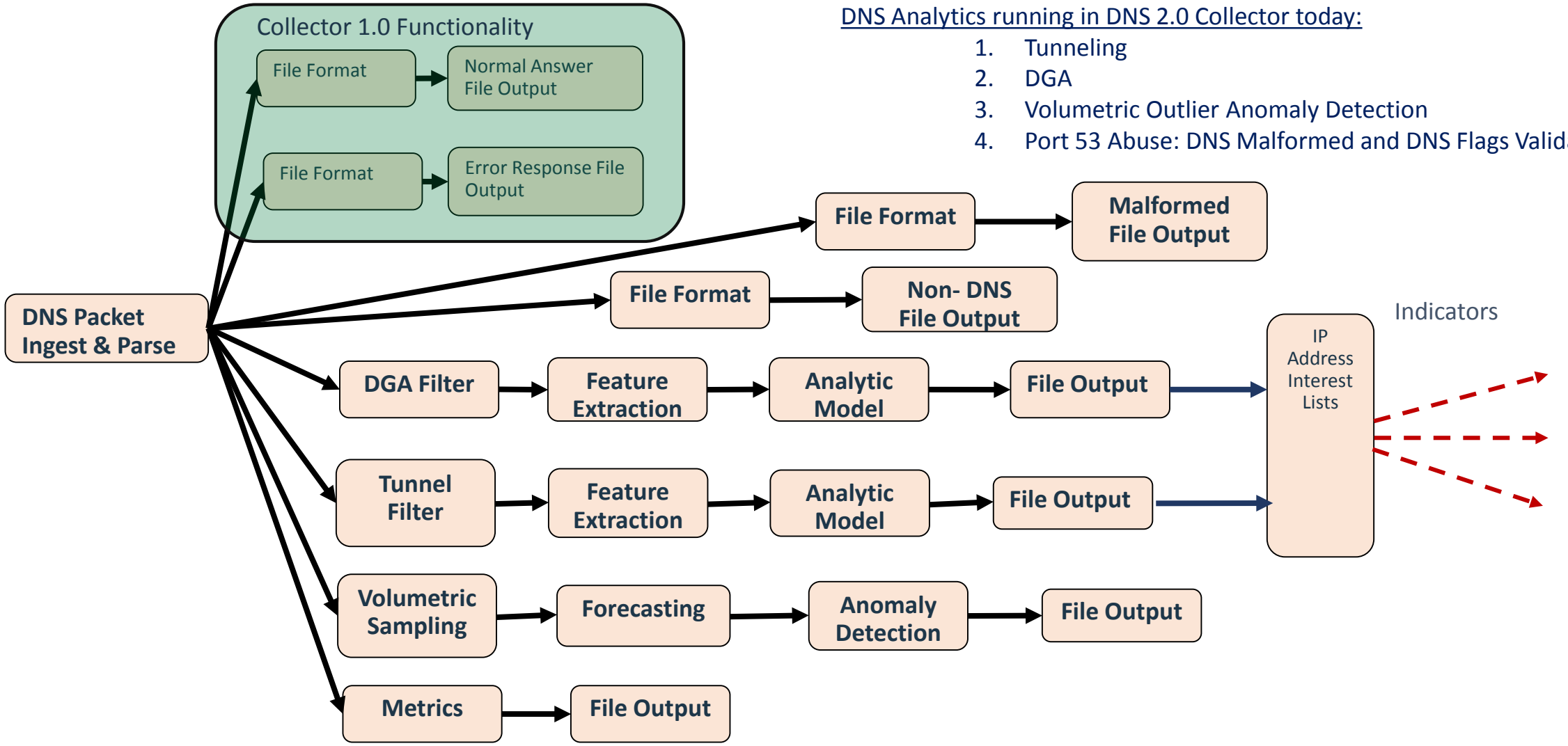
Source: AT&T DNS Collector 2.0 Feature Description

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.

Source: AT&T DNS Collector 2.0 Feature Description

DNS Collector 2.0 - Probe / Collector / Analyzer



DNS Analytics running in DNS 2.0 Collector today:

1. Tunneling
2. DGA
3. Volumetric Outlier Anomaly Detection
4. Port 53 Abuse: DNS Malformed and DNS Flags Validation

Source: AT&T DNS Collector 2.0 Training presentation

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

Weekly Cyber Threat Report

source: **http://techchannel.att.com/threattraq**