



Exceed with COLT

[Your business] exceeds with COLT

Network Response to DDoS attacks – TNC 2006

Nicolas FISCHBACH

Senior Manager, Network Engineering Security, COLT Telecom

nico@colt.net - <http://www.securite.org/nico/>

Some DDoS statistics : 1 year ago

> ~4 months

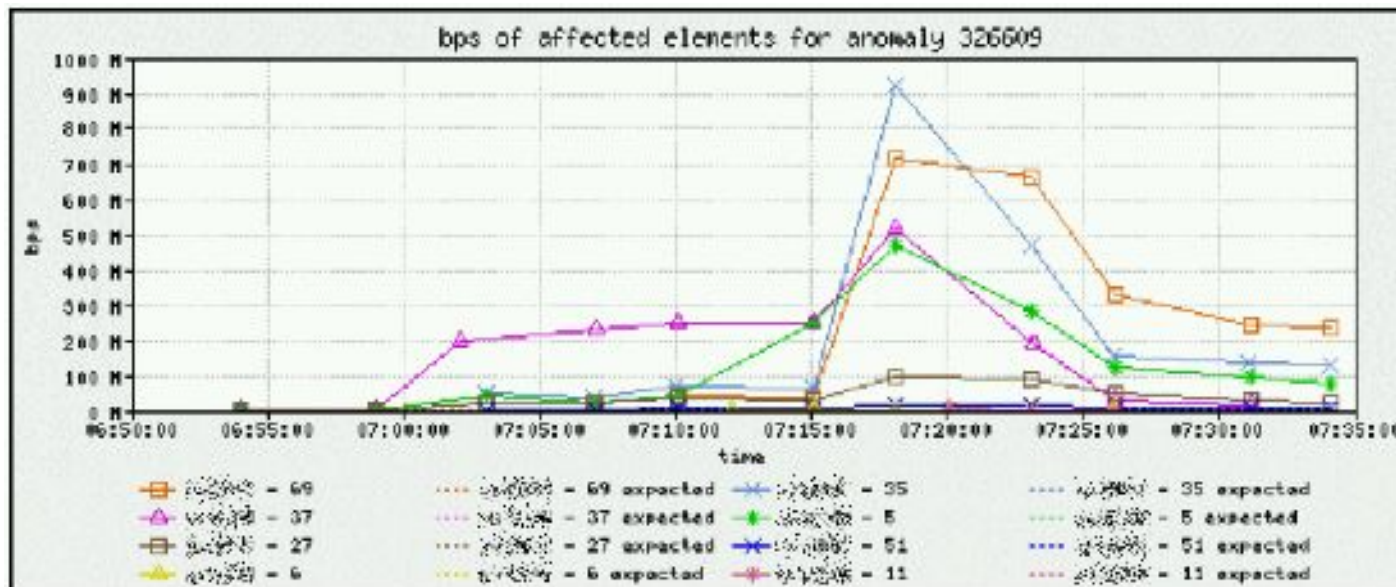
- 21962 anomalies detected
- 5302 High (“displayed”)
- 15513 Medium
- 1147 Low

> Per day

- ~40 anomalies make it to the “Security” screen in the NMC/NOC
- Some are duplicates for the same attack, some are false positives, etc.
- Overall 20 “real attacks” a day...
- A third of them are probably “business affecting” from the customer's point of view

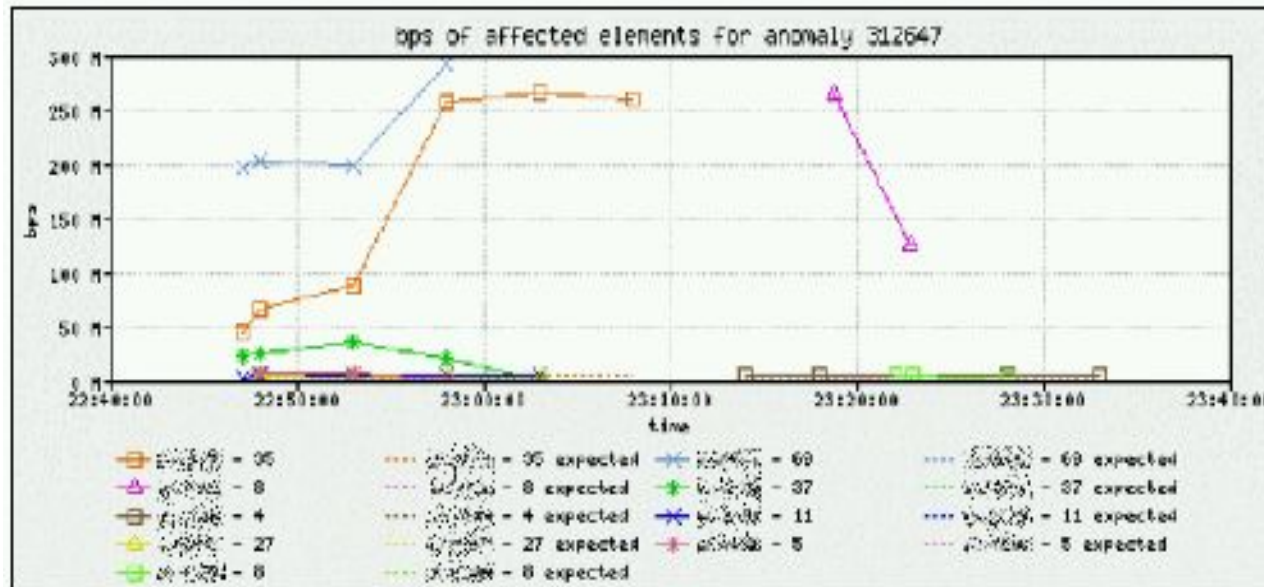
Some DDoS statistics : 1 year ago

- > Aug/13: Eat this...
 - Nearly 3Gb/s of traffic
 - Mainly from America/AP
 - 0/UDP



Some DDoS statistics : 1 year ago

> Jul/10: Let's try over different peering points



Some DDoS statistics : today

- > Why care ?
- > I'm <a large NREN> or even better, I provide capacity to large NRENs
- > I'm running a 10Gb/s core, so [censored] should I bother...
- > Well...

Some DDoS statistics : today

- > Largest DDoS attacks: 14M and 22MPPS
 - Confirmed: 9MPPS seen by one Tier1 transit
 - Towards hosting/customer, not infrastructure (except when collateral damage)
- > Most attacks in the 1-4Gb/s range (17Gb/s seen)
- > Good old TCP SYN, ICMP and UDP floods
- > Good old targets: IRC, adult, gam(bl)ing, etc.
- > Target : customer access link and DNS servers (at the same time)

Source: Danny McPherson/Arbor, H2'05 survey

Trends in botnets

- > Most botnets pretty small (in the hundreds or thousands)
- > Some really large (100K+, xM+)
- > Most common C&C is still IRC
- > But some experiments with alternative methods seen (web-based, P2P, some form of encryption and obfuscation)
- > Pretty well organized
- > Quite some firepower : but DDoS is only for “fun”, the real activities are for “profit”

DDoS detection and mitigation

- > Arbor Peakflow DoS + Riverhead-now-Cisco Guard deployed since 2002
- > Edge (peering/transit) sourced Netflow (1/100)
- > MPLS-based traffic diversion to regional Guards
- > Dedicated Guards in NYC to protect US/int'l links
- > Part of a global security project
 - MPLS core hiding
 - WRED/Engine
 - QoS
 - CoPP
 - t/i/rACLs
 - OneTACACS, OneSyslog, etc
- > 24x7 or on-demand protection

Challenges

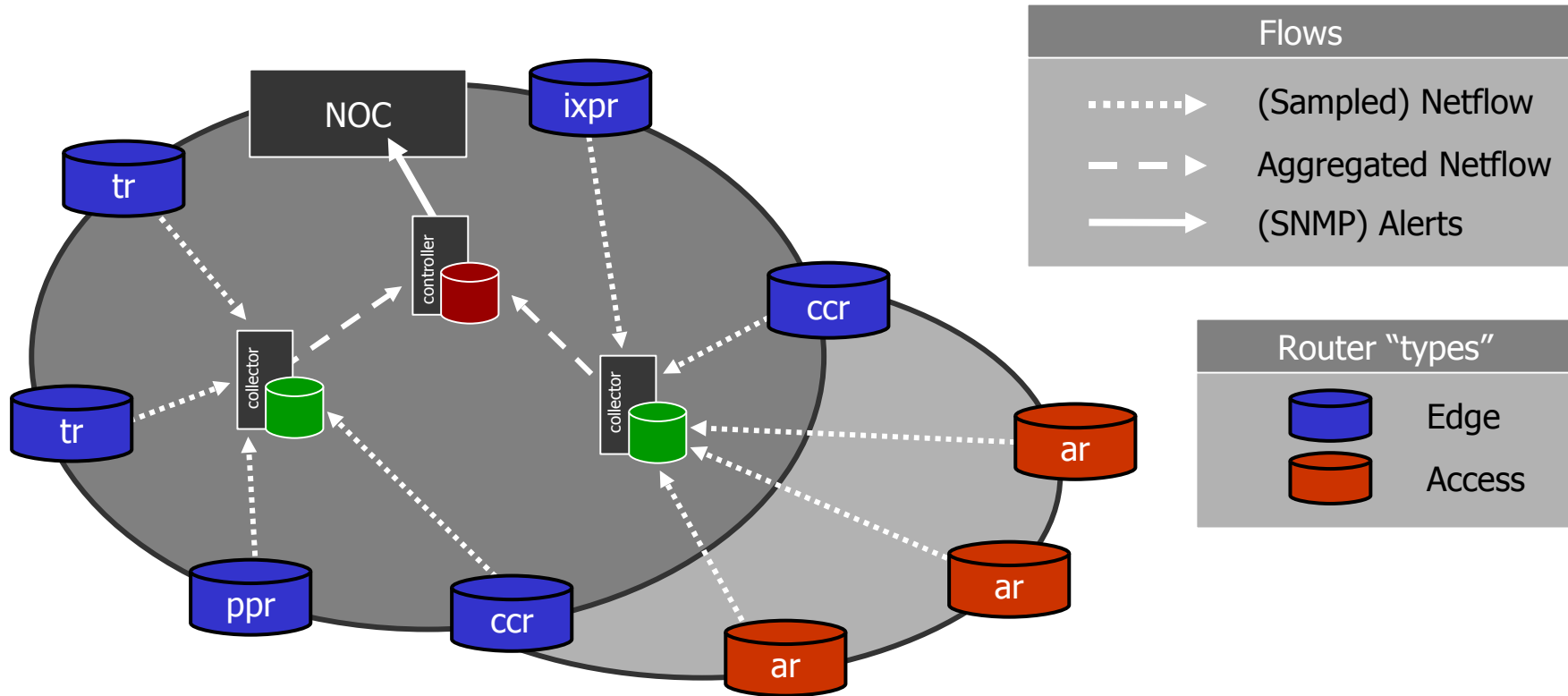
- > Security features across HW and SW platforms
- > IP routing moving closer to the CPEs (IP DSLAMs, MSPs)
- > Netflow accounting and CAPEX-scalability for access layer
- > Botnet detection vs telco license requirements (and EU regulations – 13+ countries)
- > How to enforce the AUP
- > Customers
 - Who think DDoS protection == “hacker” protection
 - Who aren't willing to understand that there's no magic solution
- > EU Data Retention Act
- > How to protect the VoIP infrastructure

DDoS detection and mitigation

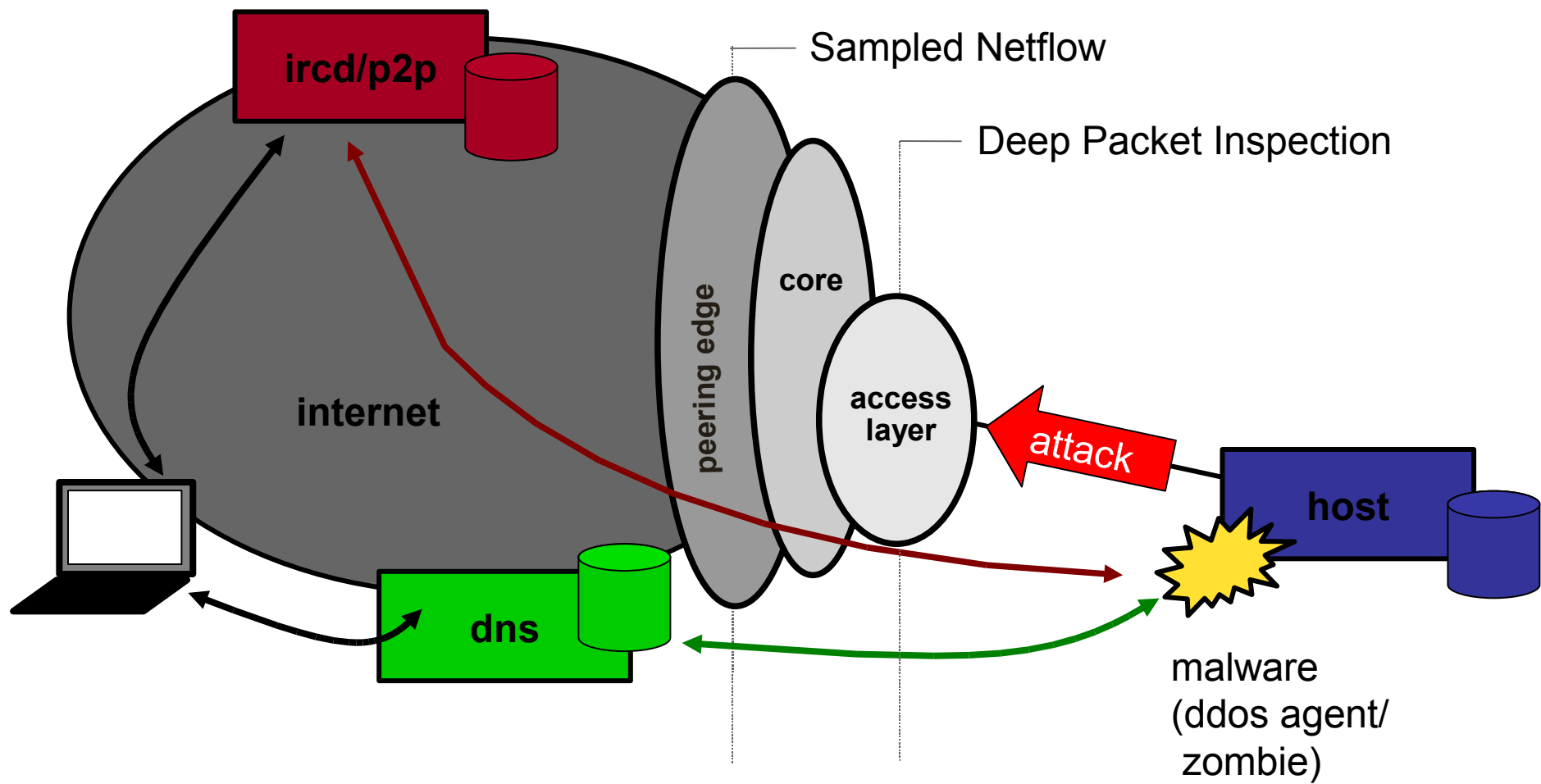
> Detection

- Most common : customer call ;-)
- Hop-by-hop traceback is so “old school”
- SNMP polling too (and not very effective either)
- Netflow

DDoS detection : Netflow



Netflow vs DPI



DDoS detection and mitigation

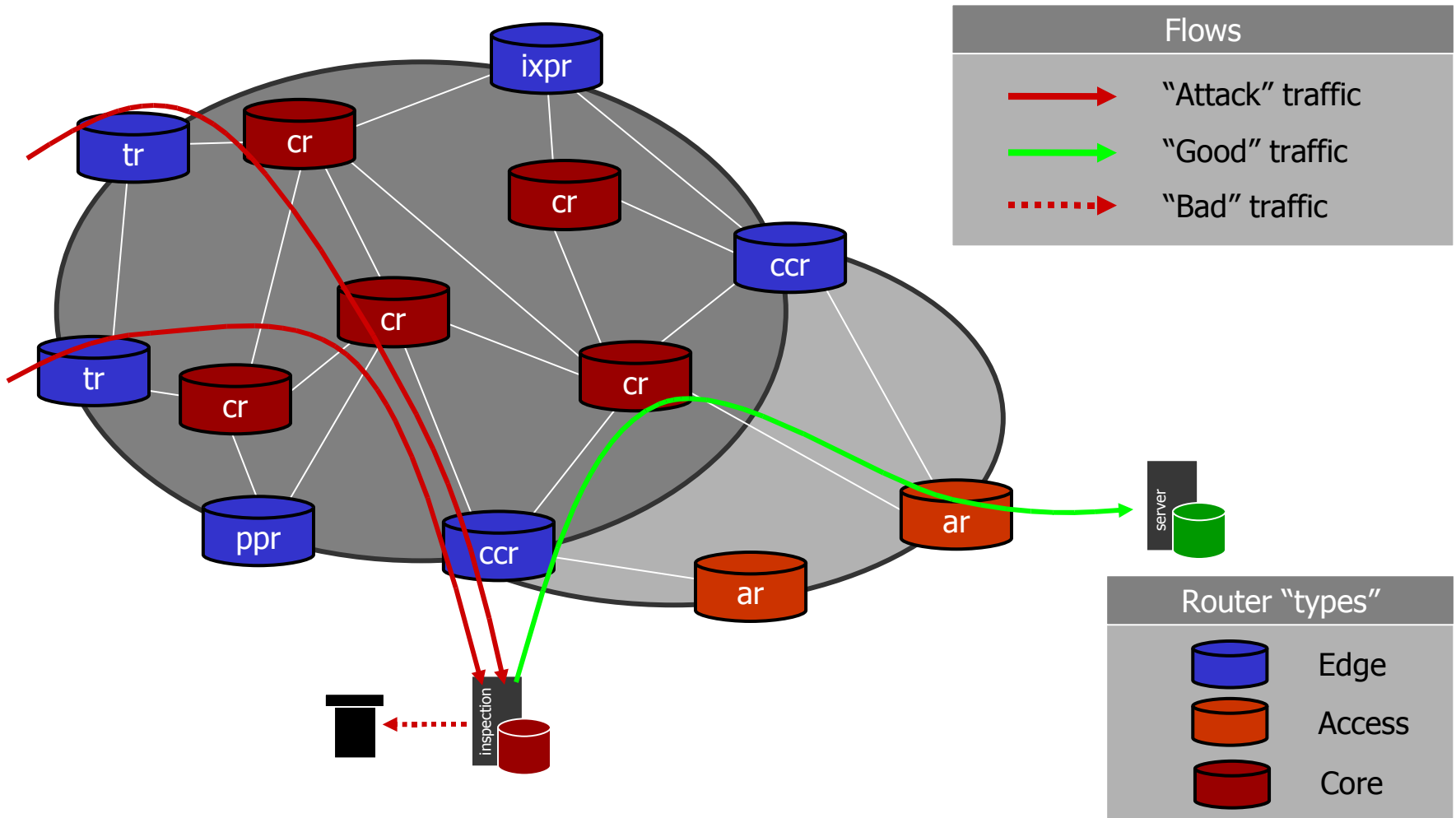
> Mitigation

- Most common :
 - BGP-based destination blackhole
 - ACLs
 - Not a fan
 - Quite some Tier1 use it
 - Depends heavily on your network structure and HW/SW capabilities
 - BGP-based source blackhole
- Diversion for scrubbing

DDoS mitigation : traffic diversion

- > Regional deployment, linked via GE to the Core and BGP sessions to Edge routers
 - IP anycast-like engineering
 - Traffic diversion using MPLS LSPs (the scrubber doesn't have to speak MPLS)
 - LSP from Edge to DCR (Directly Connected Router)
 - DCR doesn't perform a routing lookup and "sends" the IP packet to the scrubber (penultimate hop)

DDoS mitigation : traffic diversion



DDoS mitigation : traffic diversion

- > Do you need a baseline ? Helps to build a filter template
- > Inter-city spare capacity (STM-4/GE+) ?
- > No old engine cards on the divert path ?
- > No software based systems on the path ?
- > As complex to configure/fine tune than a NIDS (on a per attack basis) !
- > UDP traffic (especially DNS)
- > VoIP traffic
- > Reporting and customer “experience”

Exceed with COLT