Workflow Table Exercises

Example Table Exercises

- High-end CDMs - **.high-end**
  - Consider each of the following cases - static, PCA, and ACA
  - Example insights to consider are correlation with known protocol and known software
- Low-end CDMs - **.low-end**
  - Consider each of the following cases - static, PCA, and ACA
- Low-end CDMs and DNS queries spike during PCA - **.pca-spike**
  - Consider different affinities - ASN, IP address sources, and geo-location distribution
- Low-end CDMs and ad measurement anomaly during PCA - **.pca-ad**
  - Consider different affinities - ASN, IP address sources, and geo-location distribution
- CDMs spike during ACA - **.aca-spike**
  - Consider different affinities - ASN, IP address sources, and geo-location distribution
- Consider emergency response
  - Consider both PCA and ACA
- Something happens after granting and delegation that was not visible

TRT Report

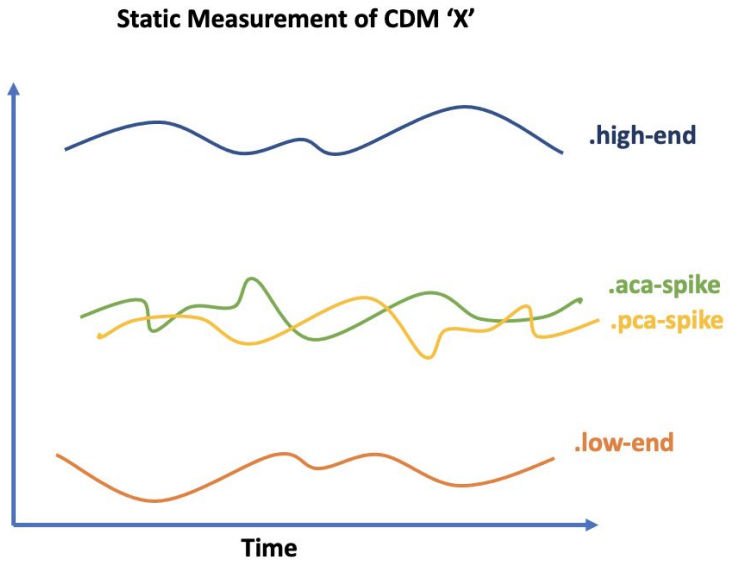
- Factual Data - present the CDMs (repeat this for static, PCA, and ACA)
  - Interpretation of the significance of each CDMs - collected either via PCA, ACA, or Third-Party Provider.
    - Query Volume
    - Query Type Distribution
    - Source Diversity - IP, Network, ASN, Geography, Open Rec vs Corp. vs ISP
    - Label Diversity - SLDs and other (Chromium, WPAD, DNS-SD, ISATAP, etc.), Regex analysis
    - Other open source intelligence
  - Interpretation of the aggregate of the CDMs
- What is the size of the “user” community impacted?
  - User is one or more of natural person, client, or service
  - Consider regional as well as global impact
- What else is notable from the CDMs collected? (open-ended question for TRT)
  - Do we get insight as to the source of the collision?
  - Do we get insight into possible mitigation or remediation strategies?
- Review any collision reports or incidents
  - Note insight regarding the impact experienced, including mitigation and remediation
- Compare and contrast this string’s CDMs with prior delegations

Data - Static List

Create a top-twenty list with our 6 names sprinkled in the list appropriately

Note that pca-ad-spike does not appear

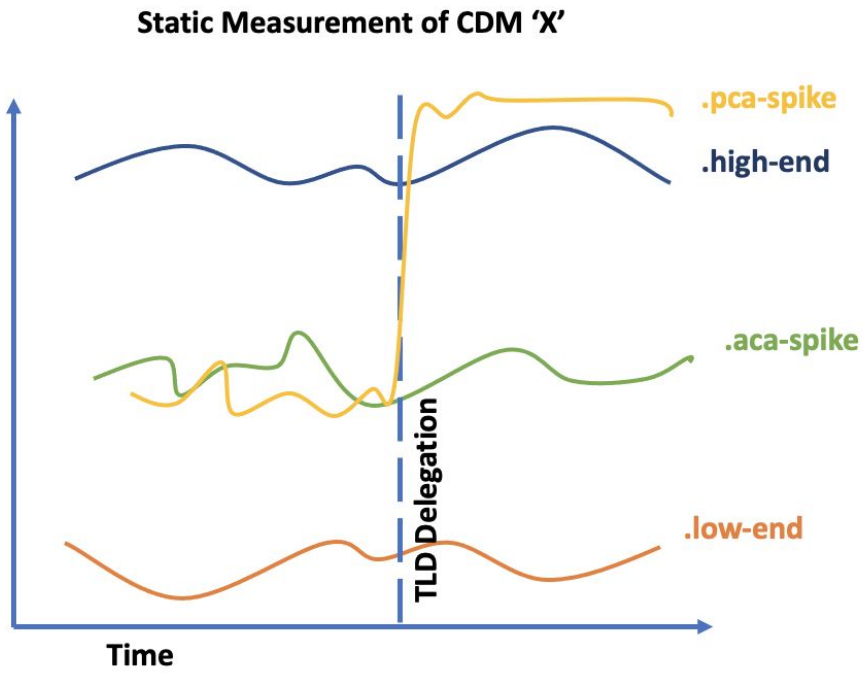
- High-end = N
- … lots of strings listed here
- Aca-spike = approx n
- Pca-spike = approx n
- Low-end = n



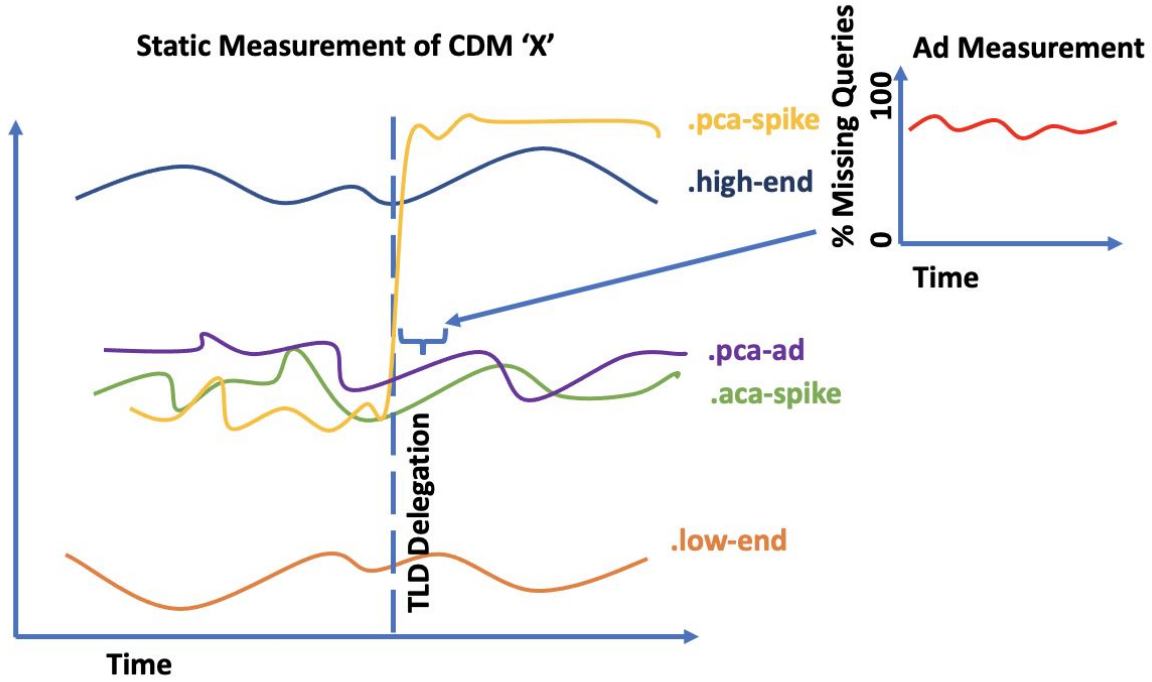
Data - PCA

PCA only

- High-end = N
- … lots of strings listed here
- Pca-spike = approx N
- … lots of strings listed here
- Aca-spike = approx n
- Low-end = n

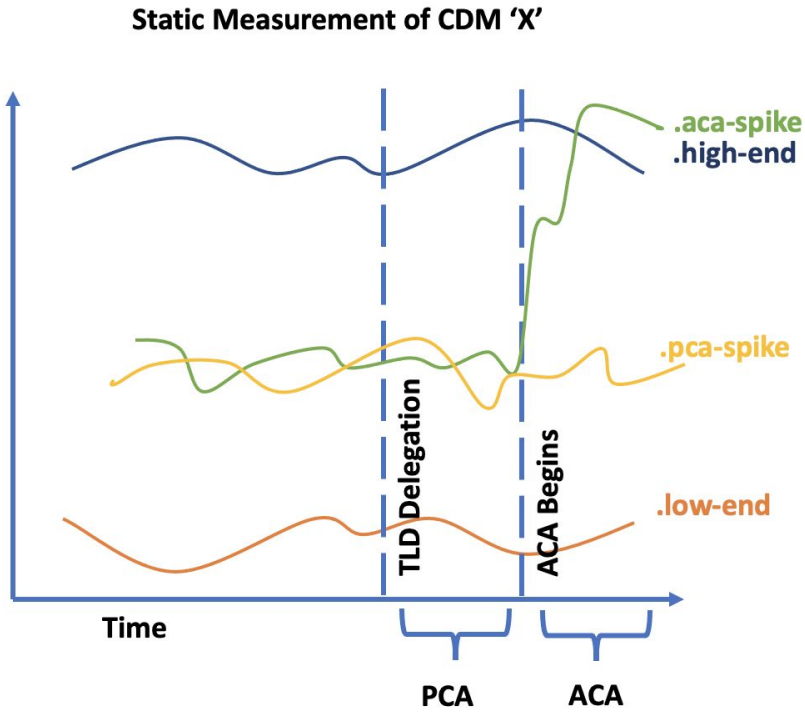


Data - PCA Ad Data



Data ACA

- High-end = N
- Aca-spike = approx N
- … lots of strings listed here
- Pca-spike = approx n
- Low-end = n



.high-end REPORT

- Factual Data
  - Static list, PCA, and ACA will all show high values for DNS
  - ACA may show some high values for other protocols
  - Diversity will be high in at least one category and perhaps others
  - Interpretation - there is a large and diverse community impacted
- Community Impact
  - For static and PCA: diversity of IP addresses is a leading indicator of the minimum size of the affected users
  - Diversity will provide an indication of regional vs global affinity
  - ACA will provide additional leading indicators based on other protocols that are instrumented
- Notable CDMs Collected
  - From the root cause report, we note that elements like WPAD might be noticed
  - A review of the labels might provide insight regarding services and software impacted
  - Each of these things could suggest mitigation or remediation strategies
- *Review any collision reports or incidents*
  - *Note insight regarding the impact experienced, including mitigation and remediation*
- *Compare and contrast this string's CDMs with prior delegations*

.low-end REPORT

- Factual Data
  - Static list, PCA, and ACA will all show low values for DNS
  - ACA will show low values for other protocols
  - Diversity will be low in all categories
  - Interpretation - there is a small community impacted
- Community Impact
  - Diversity of IP addresses is a leading indicator of the minimum size of the affected users
  - Diversity will provide an indication of regional vs global affinity
  - ACA will provide additional leading indicators based on other protocols that are instrumented
- Notable CDMs Collected
  - We would not expect any notable elements in the CDMs
  - We would not expect anything to be visible in the review of the labels
  - No mitigation or remediation strategies would be notable
- *Review any collision reports or incidents*
  - *Note insight regarding the impact experienced, including mitigation and remediation*
- *Compare and contrast this string's CDMs with prior delegations*

.pca-spike REPORT

- Factual Data
  - Static list, will show low values for DNS
  - PCA will show elevated values for DNS
  - ACA will show elevated values for DNS and maybe elevated values for other protocols
  - Diversity will be low or high in all categories
  - Interpretation - increased CDM values with lower diversity suggests a smaller and acute impact while increased CDM values with larger diversity suggests a more global and systemic impact
- Community Impact
  - Diversity of IP addresses is a leading indicator of the minimum size of the affected users
  - Diversity will provide an indication of regional vs global affinity
  - ACA will provide additional leading indicators based on other protocols that are instrumented
- Notable CDMs Collected
  - There is likely notable elements in the CDMs
  - There is likely notable insights in the review of the SLDs regarding services and software impacted
  - Mitigation or remediation strategies may be notable
- *Review any collision reports or incidents*
  - *Note insight regarding the impact experienced, including mitigation and remediation*
- *Compare and contrast this string's CDMs with prior delegations*

.pca-ad REPORT

- Factual Data
  - We get a leading indicator of the number of users
  - Diversity of various affinities: IP addresses, ASNs, and geo-location distribution
  - Diversity will be low or high in all categories
  - Interpretation - if the data aligns with PCA and ACA CDMs, this measurement is neutral
  - Interpretation - if the data is not aligned with PCA and ACA CDMs, then we have additional information about an impacted user community
- Community Impact
  - Diversity of IP addresses is a leading indicator of the minimum size of the affected users
  - Diversity will provide an indication of regional vs global affinity
- Notable CDMs Collected
  - Compare and contrast the ad data with the CDMs collected via PCA and ACA
    - There is likely notable elements
    - There is likely notable insights
  - Mitigation or remediation strategies may be notable
- *Review any collision reports or incidents*
  - *Note insight regarding the impact experienced, including mitigation and remediation*
- *Compare and contrast this string's CDMs with prior delegations*

.aca-spike REPORT

- Factual Data
  - Static list, PCA, and ACA will show low values for DNS
  - ACA will show high values for at least one other protocol
  - Diversity will be low in all categories except maybe where ACA shows new high values
  - Interpretation - there is a specific community, service, software, or protocol impacted
- Community Impact
  - Diversity of IP addresses is a leading indicator of the minimum size of the affected users
  - Diversity will provide an indication of regional vs global affinity
  - ACA will provide additional leading indicators based on other protocols that are instrumented
- Notable CDMs Collected
  - We would expect notable elements in the new high value CDMs discovered during ACA
  - Mitigation or remediation strategies may be notable
- *Review any collision reports or incidents*
  - *Note insight regarding the impact experienced, including mitigation and remediation*
- *Compare and contrast this string's CDMs with prior delegations*

Emergency Report

- The Neutral Service Provider and the TRT need to monitor delegation and any reports or incidents that manifest at all times

- Any activity that manifests a security, stability, or resiliency issue for the DNS or manifests an impact that can not be mitigated or remediated in a commercially reasonable way will be subject to an emergency response

- There must exist an authorization and method with which the TRT can request an immediate removal of the string from the root zone