

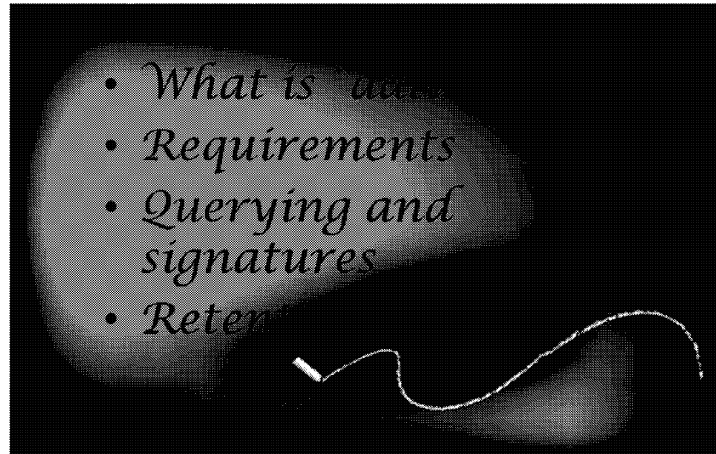
SECRET

Cyber Defence Policy Awareness Curriculum

DATA HANDLING

1

Objectives



Definitions

What is:

- Data
- Raw data
- Derivative Information

3

Before we talk about how to handle data, we need to know what “data” is.

When we say “data”, under the context of cyber defence activities conducted under Part B of CSE’s mandate, we are referring to the [REDACTED] from computer systems and networks of importance to the GC. This includes all content as well as associated metadata.

Raw data simply means data that has not yet been determined to be relevant or essential. So, once you use or retain the data, it is no longer considered raw.

Derivative information is information you get as a result of executing a malicious code. The thing about derivative information is, it is not considered data. It was not intercepted, it not PC and is therefore not subject to use or retention requirements of the MA. So, if you run some malware obtained from a PC in a virtual environment and discover that, after execution, the malware causes your system to attempt to connect to a specific domain and download a certain file, that domain and file are considered derivative information.

The best way I can explain the advantages of this are with DPSO activities. Remember back in day 1 we spoke about the different in how to share a PC in MA

vs non-MA activities? <ask someone in class to explain> So for non-MA, you need permission from the actual sender or recipient of the PC in order to share. Well, if you run the malware and get derivative information, you can now share the derivative information without the sender or recipient consent.

Definitions

Metadata

- Identifying Metadata
- Technical Metadata
- Detached Metadata

4

Metadata gets a whole slide by itself because of the sub categories. Please note, there are issues with these definitions and they are being address in future policy amendments.


So, what is Metadata? Metadata is information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content.

So basically, everything about the telecommunication that is not actual content.

For cyber defence activities under Part B of the mandate, we have identified several subtypes of metadata in an attempt to help you out conducting your activities.

Identifying Metadata is pretty self explanatory. It is metadata that could identify one or both of the communicants, or the communication itself. The idea here is, if it was obtained from or associated with a PC, then identifying metadata must be treated as a PC itself.

Technical Metadata is metadata that does not identify either of the communicant or the communication itself. So things like the version of the email protocol, or the operating system, or the internet browser version, etc. The key here is that technical metadata is not treated as a PC and is not subject to use and retention requirements.

Detached Metadata is an interesting one. The idea here is that, if metadata can be automatically separated from the associated content, there is no requirement to treat it as a PC. This metadata is considered relevant and may be kept for 

Labelling Requirements

- Client identifier
- Date/Time stamp
- Authority
- Relevant and/or essential

5

There are requirements when Data is copied/obtained/retained by CSE. Many of the labels are applied automatically by tools, but some of them you need to mark yourselves. You need to know about this as, depending on these labels, you have certain requirements on how to treat the data.

You need to know the client as this will determine whether or not you need suppressed CII in reporting.

You need to know the date/time stamp as raw data can only be kept for a limited amount of time. [REDACTED] for MA and generally [REDACTED] for non-ma.

You need to know the authority as this determines retention, as I just mentioned, as well as sharing permissions. Remember when we discussed the difference between MA and non-MA? (ask class for examples and differences in treating/sharing data).

Relevant and/or essential... we spoke about this one in part during the Private Communication lesson back in day one. Does anyone remember the requirements and how that applies to labelling? So, any data the you use and retain must be marked as relevant to Mandate B in the system. If that data happen to be a Private

Communication, it must then be determined to be and marked as essential to Mandate B. So that is your job. As you use and retain events in [REDACTED] make sure you apply the proper markings and justifications, as well as the number of PCs included in the event.

DPSO Labelling Requirements

- Private communication
- Private communication with consent to share
- Other data

6

Surprise, surprise, when dealing with OPS-1-15, Data provided by System Owner, there are additional labelling requirements for the data.

So, why do you think we need these additional labelling requirements? <ask class>

It all comes down to the intercept authority. So, for MA activities, we are allowed to intercept and use PC for the purposes of Mandate B. But, for DPSO, the system owner is intercepting data for the purpose of protecting their own networks. They can give permission to us (CSE) to share non-PC, but do not have the authority to give us permission to share PC. That authority resides with the originator or recipient of the PC itself.

SECRET

What can you do with Data?

Anything you want!*

*as long as your use of the data is in accordance with the relevant policies and authorities. Your actions cannot be directed at Canadians.

7

The fine print

*as long as your use of the data is in accordance with the relevant policies and authorities. Your actions cannot be directed at Canadians.

8

Policy is the fine print

So what's the point of those slides? Basically, to tell you that, policy doesn't tell you what you can and cannot do. What we want policy to do is show you how you can do what you want to do.

Sure, there are going to be some things that you just can't do, but I'd argue that is due to legislation, not policy.

At the end of the day, IPOC is here to support cyber defence activities and, if we can find a way to enable you to do your jobs legally, we will.

Data Querying

- Searching or scanning data
- Can be automated or manual

9

So when we say manual queries, that's when an analyst goes and enters or chooses the search criteria for their tools. Manual queries can be analysis driven, research driven or development driven.

Automated queries are when tools scan traffic based on pre-loaded criteria, scripts, signatures, etc. Automated queries can be alert driven, Anomaly driven or just set to capture certain subsets of data.

So, remember back to when I said you can do anything you want with data? Well, just remember the "can't direct at Canadian's" caveat.

So basically, you have to make sure that the criteria for your queries are not Canadian. Pretty simple right?

It does get complicated of course with spoofed e-mails, dynamic IPs and .ca domains, so how do we get around this? Focus on the foreign threat!

SECRET

Signatures

- Types

- [REDACTED]

10

Signatures are a form of automated query and are not to be directed against Canadians.

Of course, most state sponsored foreign threat actors aren't dumb and know this, so they try to use Canadian infrastructure or spoofed Canadian email to mask their origins and to launch attacks.

So, in order to help you do your job, we've introduced a new series of Signatures that allow you to include Canadian selectors.

Type 1 – Signatures that are comprised of a Canadian selector [REDACTED]

[REDACTED]

[REDACTED]

Type 2 – Signatures that are comprised of only “Canadian” selectors.

[REDACTED]

[REDACTED]



Type 1 Signatures

- Canadian Selector [REDACTED]
[REDACTED]
- Supervisor Approval
- Six month review

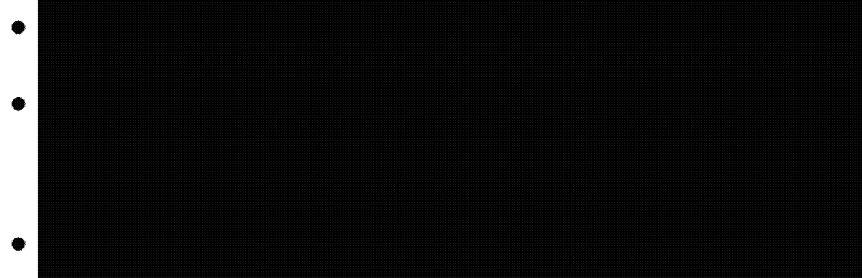
11

Once again, make sure you mark the signature as Canadian in [REDACTED] plus indicate when you've done your reviews.

IPOC must be able to access and review all the signatures.

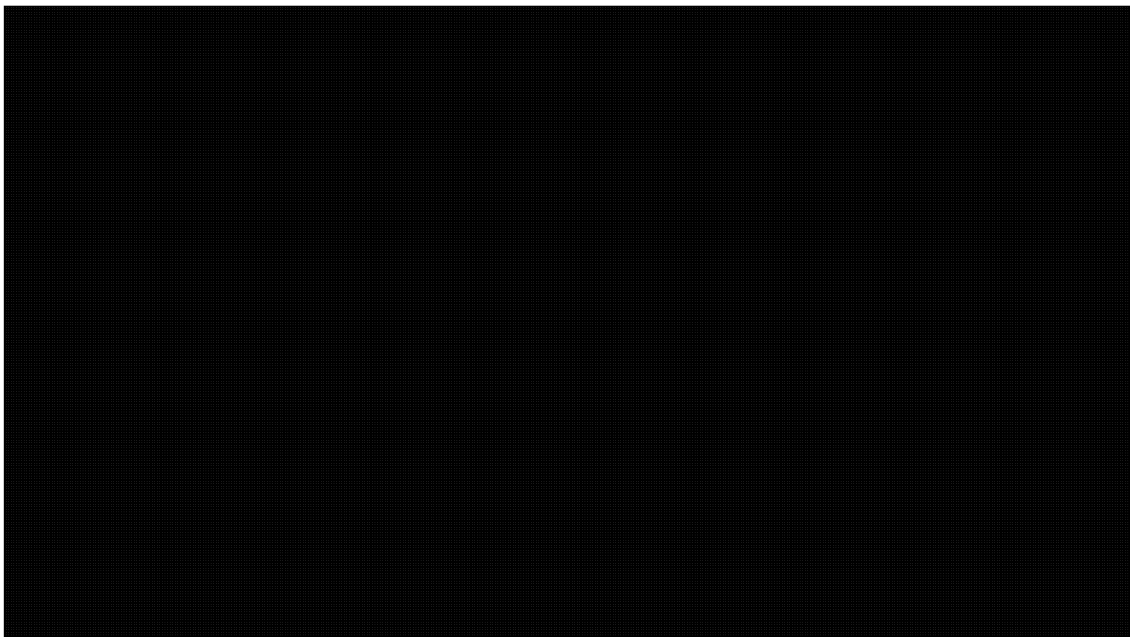
Type 2 Signatures

- Canadian Selector

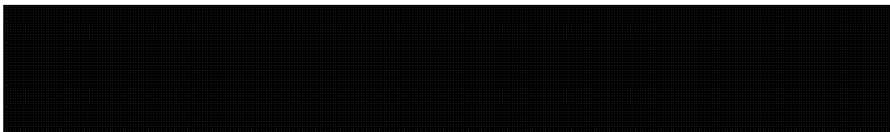


- Six month review

12



You still need to review this signature every six months.



Deletion

- Raw data MA and non-MA DPSO
- Metadata
- Local data
- Data deletion webform
- Deletion of used or retained data
- Termination of Client Arrangement

13

Raw data obtained under MA must be deleted within [REDACTED] of the date it was copied.

Raw data under DPSO (Non-MA) must be deleted within [REDACTED] of completion of the requested assistance.

Metadata can be kept for up to [REDACTED] before deletion, except if it is a PC. PC, even metadata, still has the up to [REDACTED] before deletion requirement.

In the case of our SAN, there are auto deletion scripts that handle this, so you, the operator does not have to worry about it deletion, except...

It is understandable that sometimes you need to take raw data and save it onto your local workstation/desktop in order to conduct analysis. This is fine, except you have to remember to delete the data in the required amount of time. Every quarter, regardless if you save data locally or not, if you are part of the raw data access list (ALPR) you must fill out the webform confirming that you have verified your local workstation and deleted any required data. IPOC sends out quarterly reminders with the webform link to the entire ALPR dist list, so just make sure you do it.

If you've retained data and later on determine that it no longer is relevant/essential,

it can be deleted. A Cyber Defence supervisor must approve the deletion, and IPOC informed to ensure that any stats for reports are correct.

Also, if a client arrangement is being terminated, any used and retained data can still be kept as per CSE retention and dispositions schedules. Any copied, selected or intercepted data must be deleted within [REDACTED] days from the notification of suspension/termination of the arrangement, or one year from the date the data was copied, whichever comes first.

Retention

- Used or retained
- Relevant or essential
- Data and reports
- Metadata

14

Raw data may be marked as used or retained if you deem it relevant or essential to Mandate B.

Can anyone explain the difference between Relevant and Essential in this context?

Relevant = provide advice, guidance and services to help ensure protection

Essential = identify, isolate or prevent harm

Can only retain PC if it is essential.

You do not have to write a report if you want to retain data. Translation, you can retain data without putting it in a report.

On the flip side, any data used in a report must be retained for as long as the report is retained.

Metadata that is used and retained is treated the same as regular data. Raw metadata has a shelf life of up to [REDACTED] before deletion.

Exception, metadata used only to generate statistics or to show trends is not subject to use and retention policy.

Exception 2 – Identifying metadata must be treated as a recognized PC and therefore can only be kept for up to [REDACTED] before deletion or retention.

SECRET



15