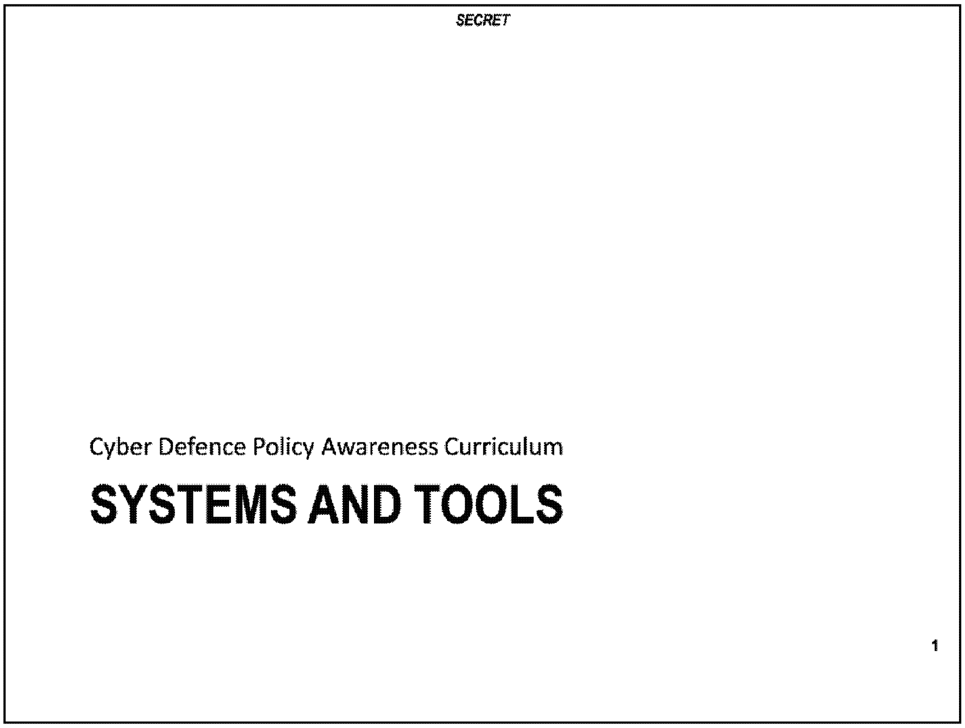
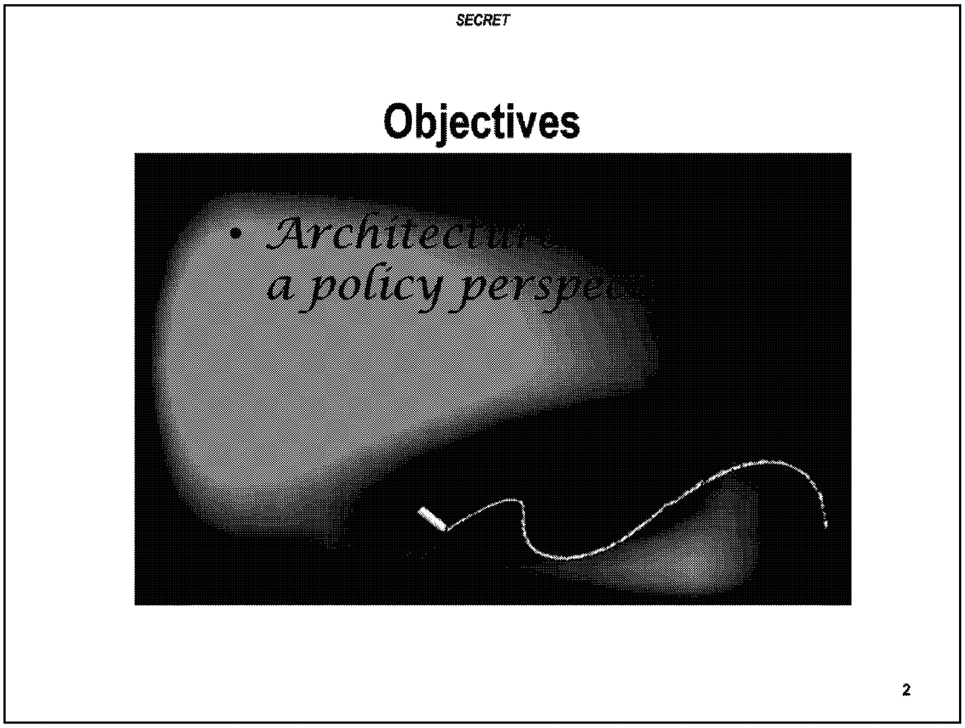


SECRET

Cyber Defence Policy Awareness Curriculum

SYSTEMS AND TOOLS



SECRET

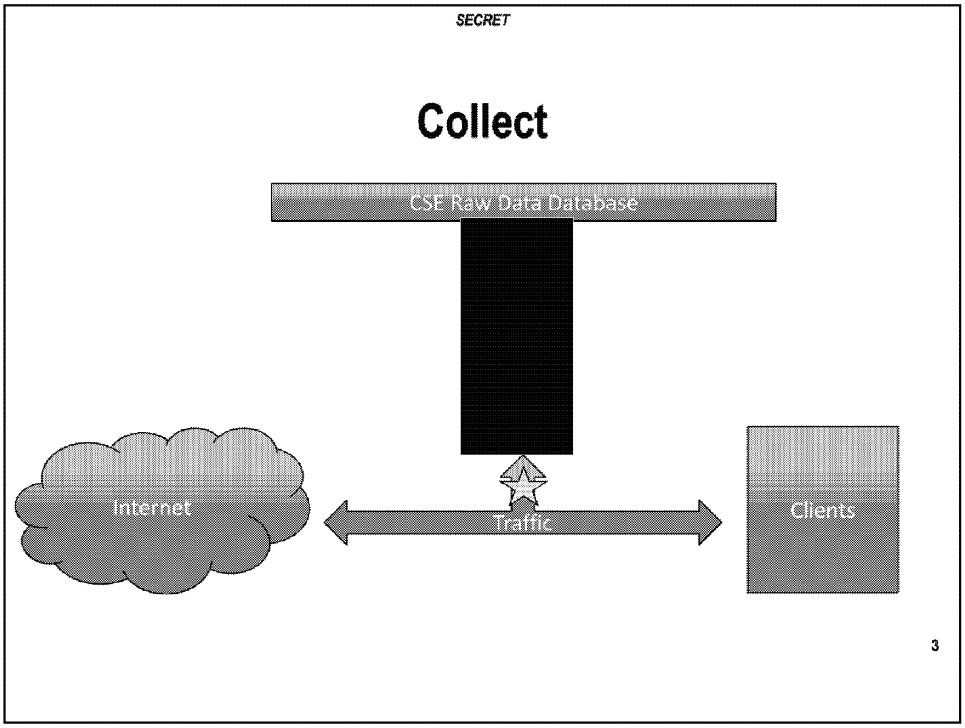
Objectives

- *Architectu*
  a policy perspec

2

Remember, all this is from a policy perspective, so ignore the glaring technical inaccuracies and omissions.

The aim of this lesson is to graphically show you how the major policy concerns fit into the system architecture and your day to day activities.



SECRET

Collect

CSE Raw Data Database

[redacted]

Internet

Traffic

Clients

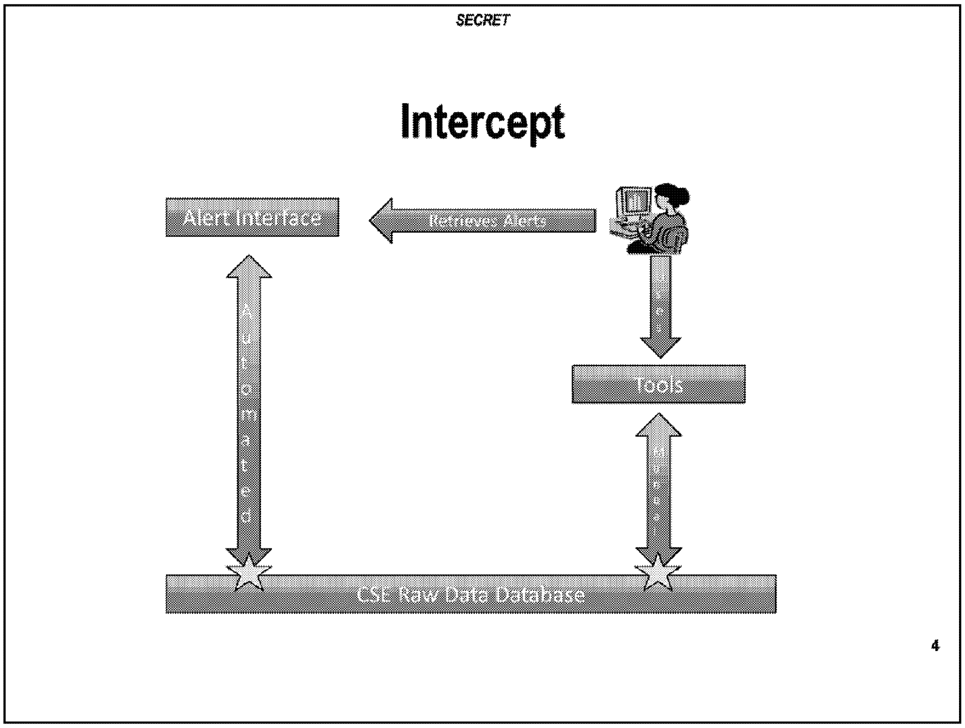
3

The concept of “collect” is an important one because, it’s how we get our MA data.

Basically, all traffic that passes through our [redacted] is automatically collect and sent to our Raw Data Database (a.k.a [redacted]

Note – Yes there may be black/white listing or firewalls applied at this time, but for policy purposes, this collect is treated as unaltered and unselected data. It is not targeted, it is a bulk collect of “everything”.

So now that we have the raw data, what is the next step?



SECRET

Intercept

4

The point of interception happens when selectors are applied against the collected raw data.

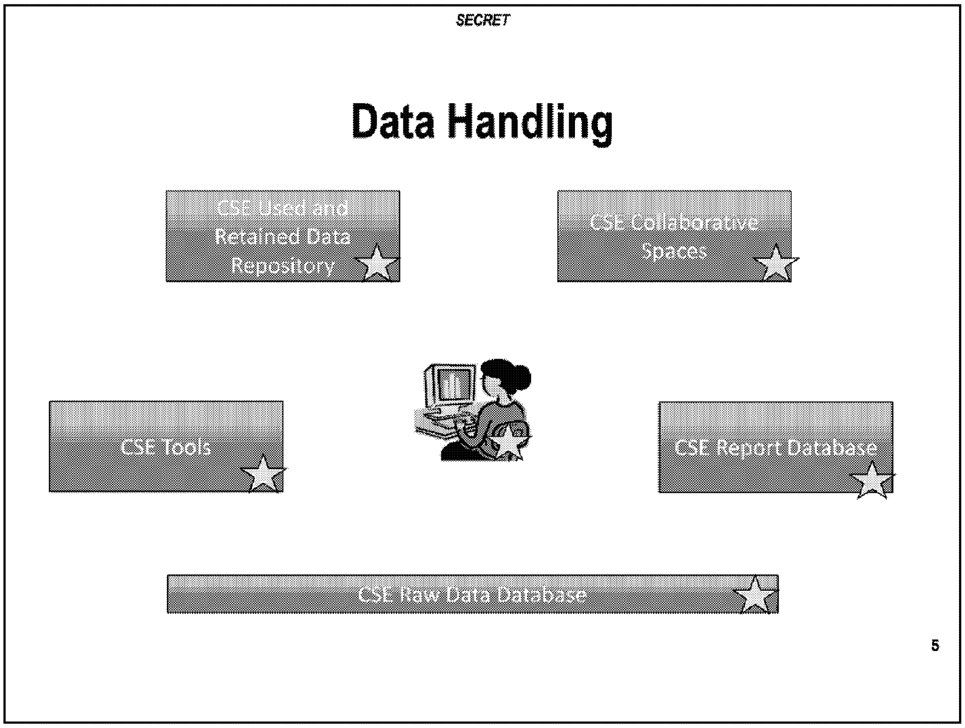
Remember, although the term selector is normally associated to SIGINT, applies to us in ITS as well. Simply put, “selectors” are any alpha numeric string that is applied against data to identify or isolate it for further processing/analysis. Selectors can include, but are not limited to, e-mails, names, IPs, [redacted]

So collected data (as seen in the previous slide) has not yet been intercepted.

We’ll go into more detail in a future lesson, but essentially, data can be intercepted manually or by an automated process. In the manual case, the analyst uses her tools and applies her selectors against raw traffic.

In the automated case, selectors are applied automatically via things through pre-loaded/determined criteria, like signatures.

In both cases, the interceptions happens before the analyst even see what data was returned/selected.



SECRET

Data Handling

CSE Used and Retained Data Repository

CSE Collaborative Spaces

CSE Tools

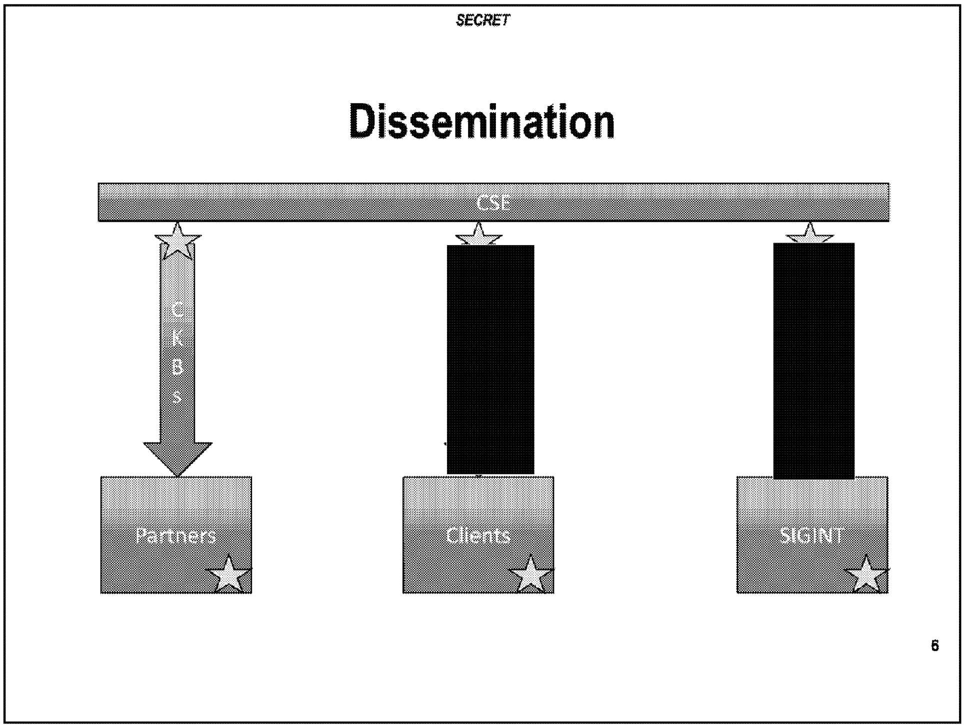
CSE Report Database

CSE Raw Data Database

5

Data gets used, stored, analysed and manipulated in many different ways and in many different locations and we have the responsibility to ensure that it is always treated correctly.

Depending on the type of data, the function of the tool or database and who has access, data handling requirement vary greatly. Don’t worry though, we are gong to go through all the good stuff in the upcoming modules. The aim of this is just to show you how data handling policies fit into the big picture.



SECRET

Dissemination

CSE

CKBS

[redacted]

[redacted]

Partners

Clients

SIGINT

6

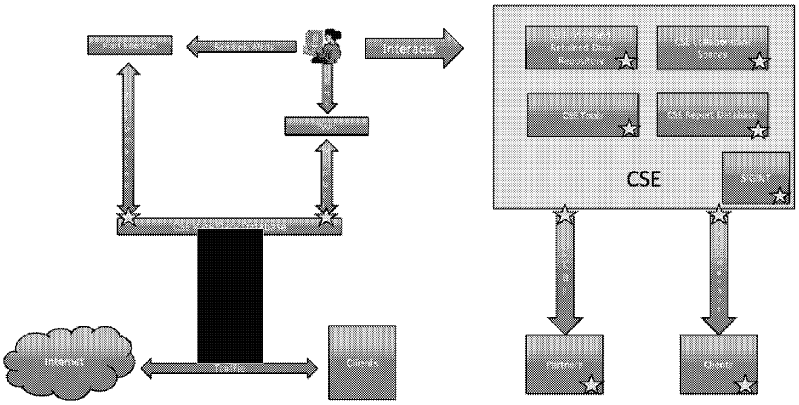
Finally, how do we get the information out to the appropriate audience? What can we give them?

And once they get it, what can they do with it? Do we even care?

All these issues will be covered we get further into the course, but what I want you to remember is: it's not what the tool is or what it is called that matters. It's what it is supposed to do with the data that matters.

SECRET

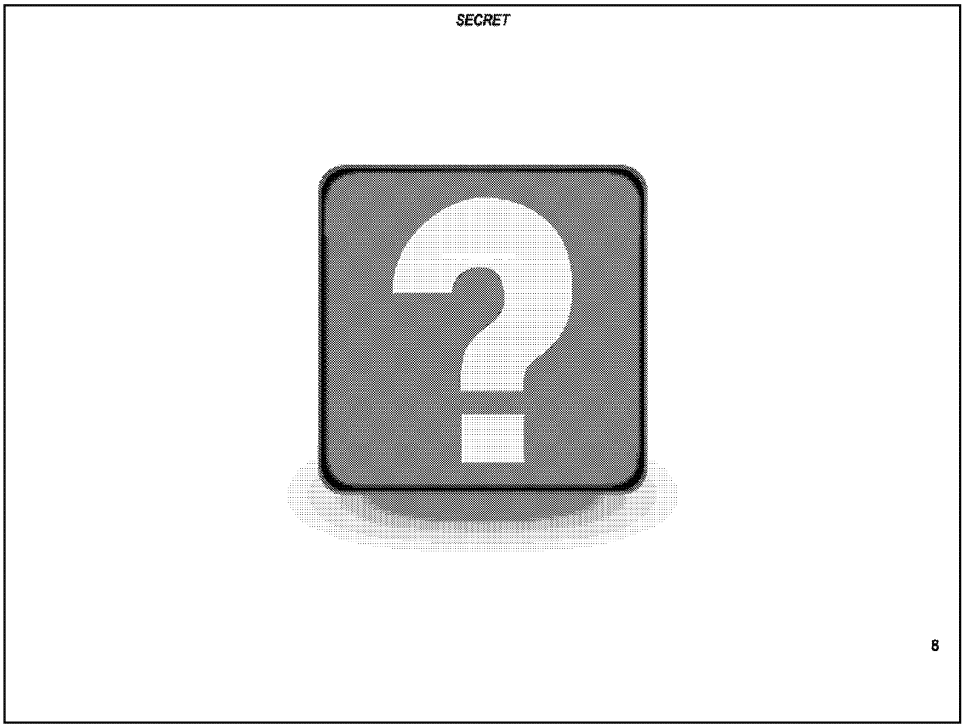
Consolidated slide



[redacted]

7

And here's what it looks like all together.



SECRET

8