

Certify Security?

Al Potter

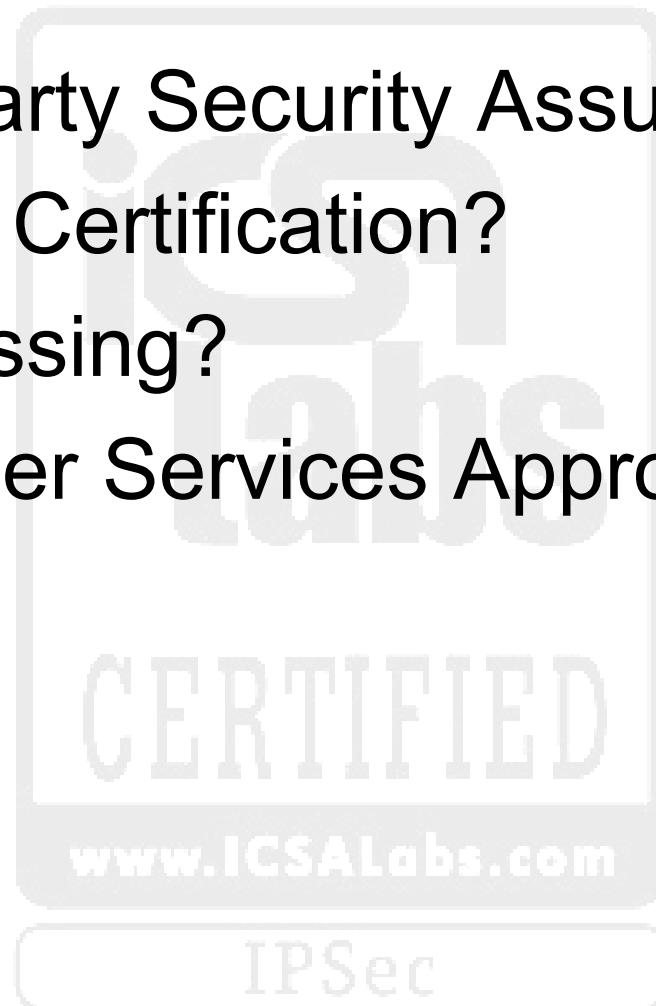
Premier Services Labs Manager

ICSA Labs

apotter@icsalabs.com, PGP Key ID: 0x58C95451

IPSec

- Why 3d Party Security Assurance?
- What –IS- Certification?
- What's Missing?
- The Premier Services Approach



Why 3d Party Assurance?

Vendor:

“Trust me, it’s secure.”

Customer:

“OK!” (Doh!)

or

“Yeah, Right....”

or

“Secure? Whassat?”

Reagan:

“Trust, but Verify....”

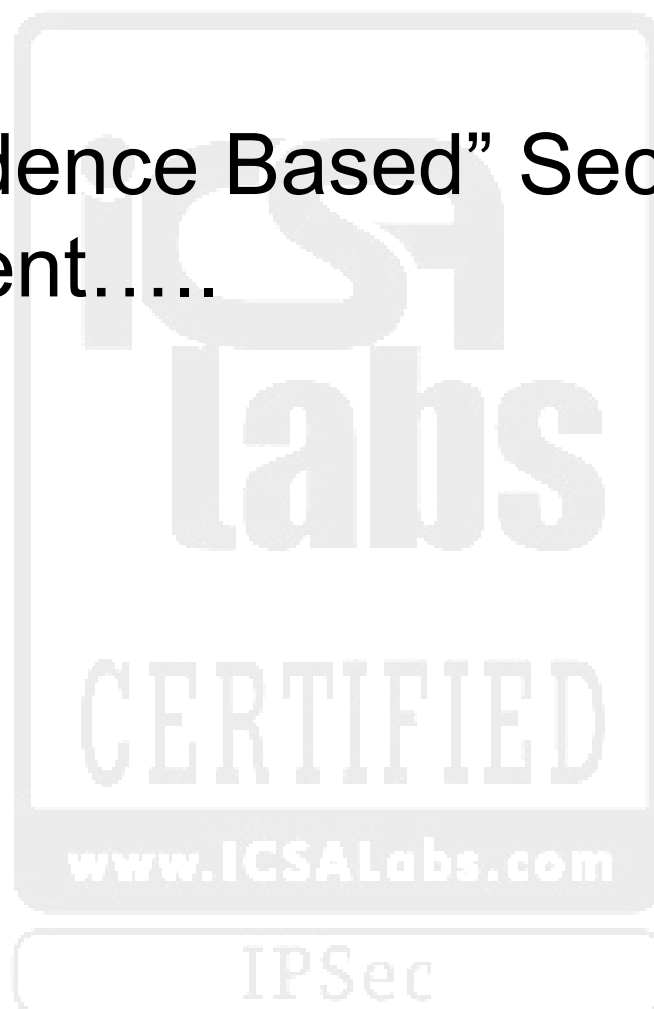


(Generic) Certification

- A performance standard is set.
- Test Methods are established.
- Product is evaluated, producing evidence.
- Evidence is presented; a decision is made as to whether the evidence supports the conclusion that the product meets the standard.
- If it does, Somebody issues a Certificate.

Certification, Cont'd

This is “Evidence Based” Security
Assessment.....



What's Missing?

- “Certification” is (supposed to be) Objective, Black and White.
- This doesn't fit a lot of today's security problems:
 - Spam
 - Spyware
 - Anything where vendor reaction time is an issue.
- The “Snapshot” Problem

Premier Services

- Certify what we can
- Evaluate the rest
- Compare where possible

In the end, you have more assurance than before.....

