OSSTMM V 2.1

Eduardo Jorge Feres Serrano Neves eth0

www.h2hc.com.br

ISECOM

- **O que é?**

  Instituto para Segurança e metodologias abertas.
- **Qual a proposta?**

  Pesquisa e conscientização na área da Segurança
- **Qual a área atual de atuação?**

  EUA, EUROPA

OSSTMM

- **Um pouco de história**: a OSSTMM foi criada com intuito de apenas citar normas e metodologias para a comunidade de segurança, mas, como obteve um grande sucesso, hoje ela ja conta com duas certficações válidas: OSSTMP e OSSTMA, e seu reconhecimento atravez do mundo todo.

OSSTMM

- **Em que consiste?**

  - Padrão profissional para testes de segurança
- **Qual o objetivo ?**

  - Criar metodologias para testes de segurança
- **Publico Alvo?**

  - Profissionais de área de segurança ou pessoas com conhecimentos na área

OSSTMM

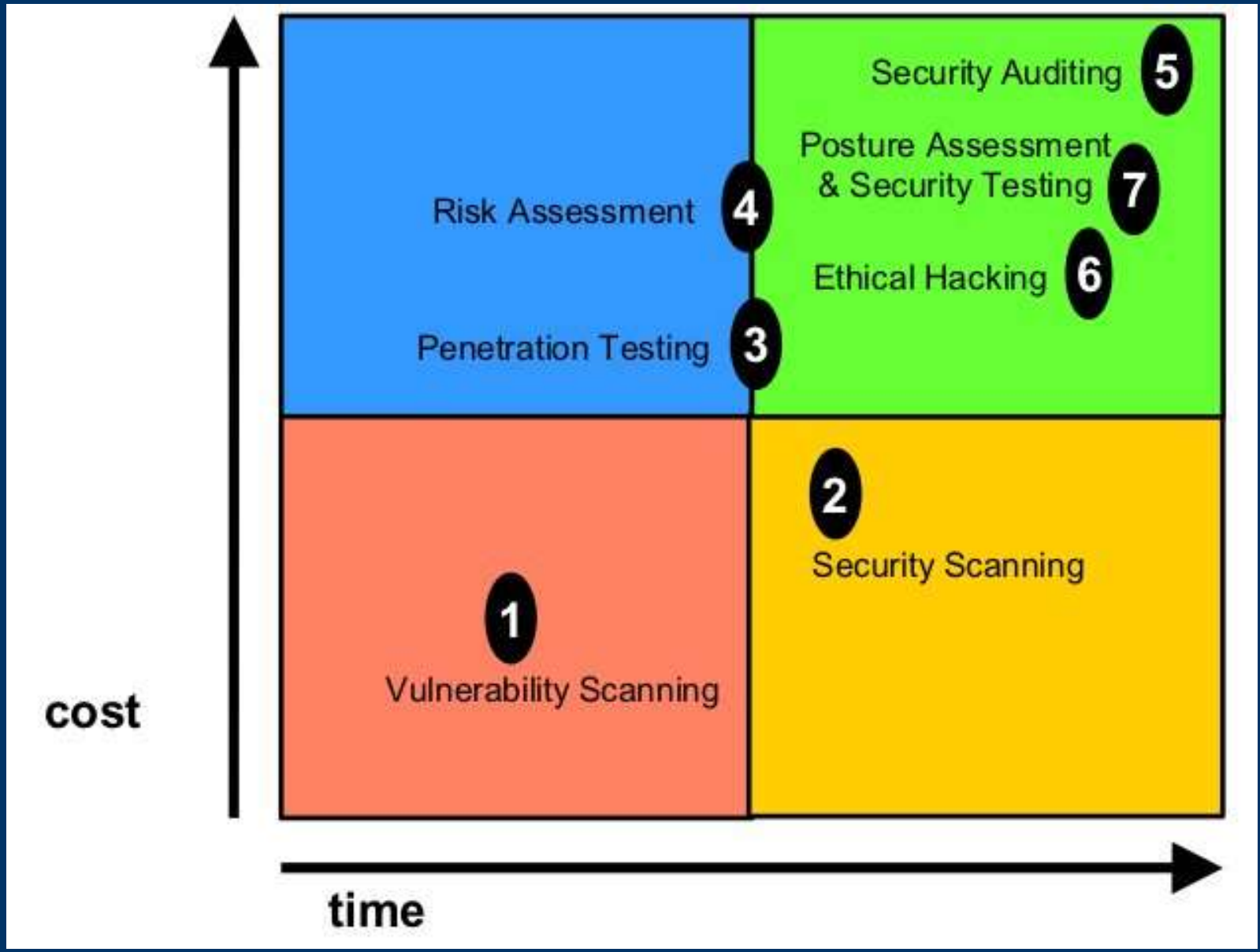
- **Validade do teste?**

  - Deve seguir alguns padrões para ser considerado pelo ISECOM

Padrões do ISECOM

- Quantificável
- Baseado em análises, e não em marcas comerciais
- Consistente e repetido
- Exaustivo
- Válido além do momento do teste
- Concordante com as leis locais

TEMPO X CUSTO



TEMPO X CUSTO

- Escaneamento de vulnerablidades
- Escaneamento de segurança
- Teste de penetração
- Avaliação de riscos
- Auditoria de Segurança
- Hacking Ético
- Avaliação de Posturas

CORRESPONDECIA LEGAL

- Segue normas e leis para o direito digital criadas pelos países
- **Austria**

  - Austria Data Protection act 2000
- **USA**

  Federal Information Security Management act.
  USA Government Information Security Reform
  Children's Online Privacy Protection act (COPPA)

CORRESPONDENCIA LEGAL

- **Alemanha**

  Deutsche Bundesdatenschutzgezets (BDSG)
- **Espanha**

  Spanish LOPD ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal Art. 15 LOPD – Art 5

  LSSICE

CORRESPONDENCIA LEGAL

- **Canadá**

  Corporate Governance

  Provincial Law of Quebec, Canada Act Respecting the Protection of Personal Information in the Private Sector(1993)
- **Reino Unido**

  UK data Protection Act 1998

  Corporate Governance

CORRESPONDENCIA LEGAL

- **Austrália**

  Privacy Act Amendments of Australia

  National Privacy Principle(NPP)

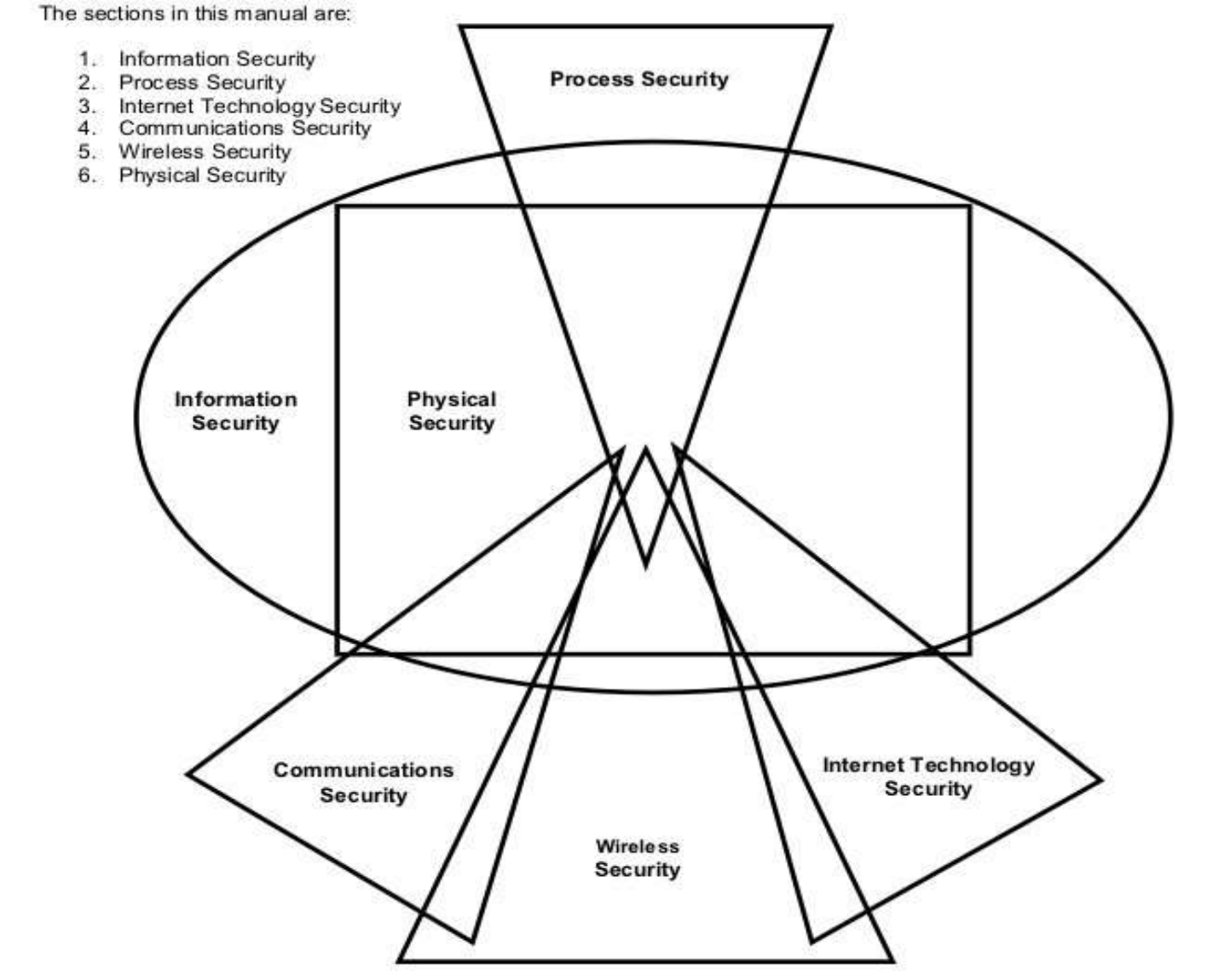
EQUIVALÊNCIAS

- IT Information Libary
- Germany: IT Baseline Protection Manual
- German IT Systems
- ISO 17799-2000
- GAO/FISCAM
- SET
- NIST
- MTRE

Processos

- Visibilidade
- Acesso
- Confiança
- Autenticação
- Não Repúdio
- Confidenciabilidade
- Privacidade
- Autorização
- Integridade
- Segurança
- Alarme

MAPA DA SEGURANÇA



MAPA DA SEGURANÇA

- **Segurança da Informação**
  - Avaliação de Postura
  - Integridade da Informação
  - Exame de Inteligencia
  - Revisão da Inteligencia Competitiva
  - Recursos Humanos
  - Politicas de Controle
  - Controles de Informação

MAPA DA SEGURANÇA

- **Processo de Segurança**
  - Revisão de Posturas
  - Analisando Requisição
  - Analisando Sugestões
  - Analisando Pessoas Confiaveis

MAPA DA SEGURANÇA

- **Segurança na Internet**
  - Logistica e controle
  - Revisão de politicas
  - Revisão de detectores de instrusão
  - Levantamento da Rede
  - Identificação dos Serviços do Sistema
  - Busca de Informações Competitivas
  - Revisão da privacidade
  - Coleta de dados

MAPA DA SEGURANÇA

- **Segurança na Internet (cont)**
  - Teste de aplicações para internet
  - Busca e verficação de vulnerabilidades
  - Roteamento
  - Teste de sistemas seguros
  - Teste de controle de acesso
  - Quebra de senhas
  - Medidas de contingencia
  - Teste de negação de serviço (Dos)

MAPA DA SEGURANÇA

- **Segurança na Internet (cont)**
  - Revisão das politicas de segurança
  - Revisão de alertas e logs

MAPA DA SEGURANÇA

- **Segurança da Comunicação**
  - Revisão de posturas
  - Teste de PBX
  - Teste de correios de voz
  - Revisão dos FAX
  - Teste dos modems

MAPA DA SEGURANÇA

- **Segurança Wireless**
  - Revisão de posturas
  - Verificação de radiação eletromagnetica
  - Teste de redes Wireless 802.11
  - Verificação de redes Bluetooth
  - Verificação dos dispositivos de entrada Wireless
  - Verificação de Handheld Wireless
  - Verificação das comunicações sem cabo
  - Teste dos dispositivos de segurança sem fio

MAPA DA SEGURANÇA

- **Segurança WireLess (cont)**
  - Dispositivos de transação sem fio
  - Verificação da RFID
  - Teste de sistemas infravermelho
  - Revisão de privacidade

MAPA DA SEGURANÇA

- **Segurança Fisica**
  - Verificaçaõ de controles de acesso
  - Revisão do perimetro
  - Revisão de monitoramento
  - Verificação das respostas dos alarmes
  - Revisão do local
  - Revisão do entorno

Avialiação de riscos

- Segurança
- Privacidade
- Praticidade
- Usuabilidade

Segurança "perfeita"

- **Serviços e acesso a internet**
  - Não usar acesso remoto sem criptografia
  - Não usar acesso remoto sem autenticação
  - Restingir tudo liberar apenas o especifico
  - Monitorar e logar tudo
  - Descentralizar
  - Limitar a confiança entre sistemas
  - Colocar em quarentena as entradas e valida-las

Segurança "perfeita"

- **Serviços de acesso a internet (cont)**

  - Instalar somente aplicações/serviços necessarios
  - Dividir a segurança em camadas
  - Seja invisivel mostra somente o necessario
  - A simplicidade previne erros de configuração

- **Computação movel**

  - Colocar em quarentena todos as entradas de rede e todo o trafego da rede

Segurança “perfeita”

- **Computação movel (cont)**
  - Não usar acessos remotos descriptografados
  - Não usar acessos remotos sem autenticação
  - Criptografia de acordo com as necessidades
  - Instalar somente aplicações/ serviços necessarios
  - E melhor ser invisivel sem serviços rodando
  - Exigir senhas de BIOS
  - Treinamento de segurança

Segurança “perfeita”

- **Aplicações**

  - O uso de caracteristicas de segurança deve ser obrigatorio
  - Ajustar as regras de negocio para entradas e saidas da apliação
  - Validar todas as entradas
  - Limitar as confianças (Sistemas e Usuarios)
  - Criptografar dados

Segurança “perfeita”

- **Aplicações (cont)**
  - Criptografar todos os componentes
  - Todas as acões ocorrem do lado do servidor
  - Definir camadas de segurança
  - Seja invisivel, mostre somente o seu serviço
  - Acionar alarmes

Segurança “perfeita”

- **Pessoas**

  - Autoridade descentralizada
  - Responsabilidade pessoal
  - Segurança pessoal e controles de privacidade
  - Treinamente e definiçao de leis e éticas para politica de segurança
  - Acesso a informações e infraestrutura limitados

Valores da avaliação de riscos

- **RAVs**
- **Definições dos RAVs**

  1 – Grau de degradação de cada modulos individual

  2 – Definição de um ciclo de tempo

  3 – Tem influencias de outros modulos?

  4 – Estabelecer pesos

  5 – Tipo, identificado, verificado e não aplicado

Tipos de riscos

- Vulnerabilidade
- Fraquezas
- Filtragem de informação
- Preocupação
- Desconhecidos

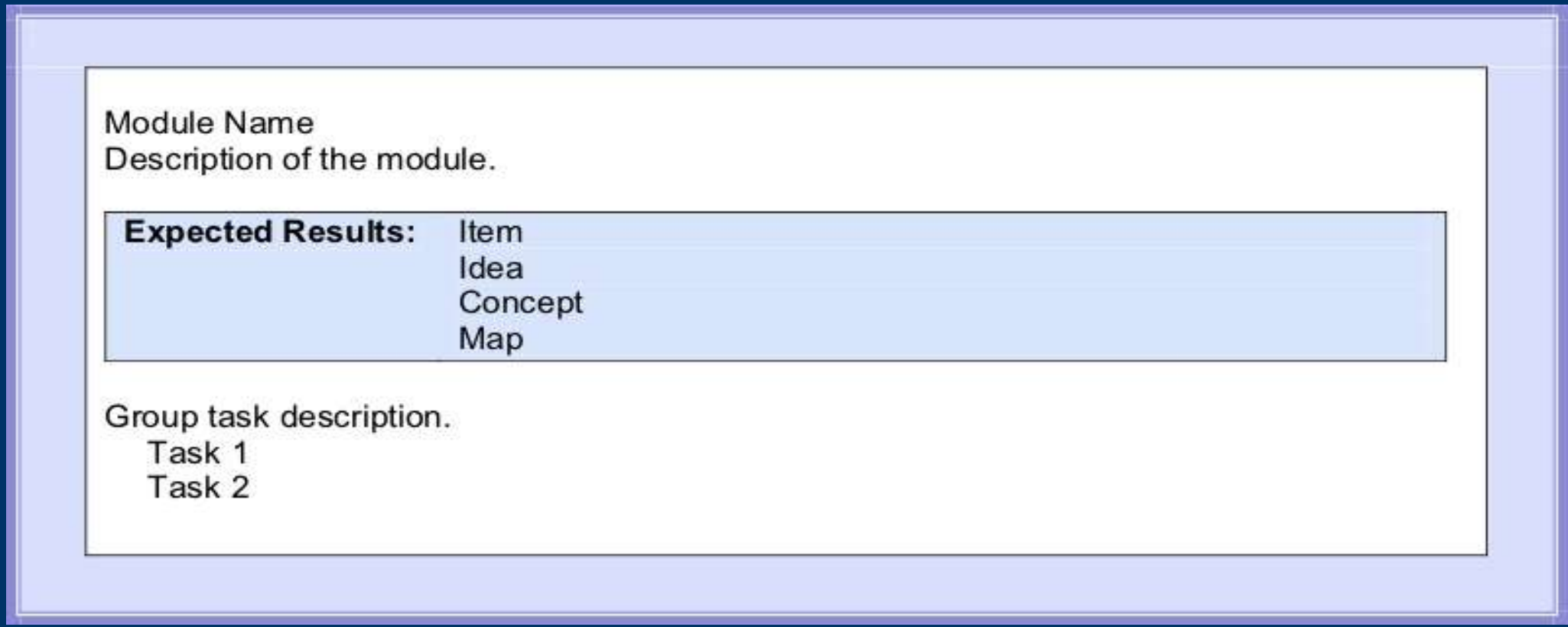
	Verified	Identified	Not Applicable
Vulnerability	3.2	1.6	0.4
Weakness	1.6	0.8	0.3
Concern	0.8	0.4	0.2
Information Leak	0.4	0.2	0.1
Unknown	0.2	0.1	–

Sessões e Módulos

- A metodologia e dividida em módulos, sessões e tarefas
- Sessões são os pontos do mapa da segurança
- Módulo e o fluxo da metodologia
- Tarefas são entradas e saídas de dados dos Módulos

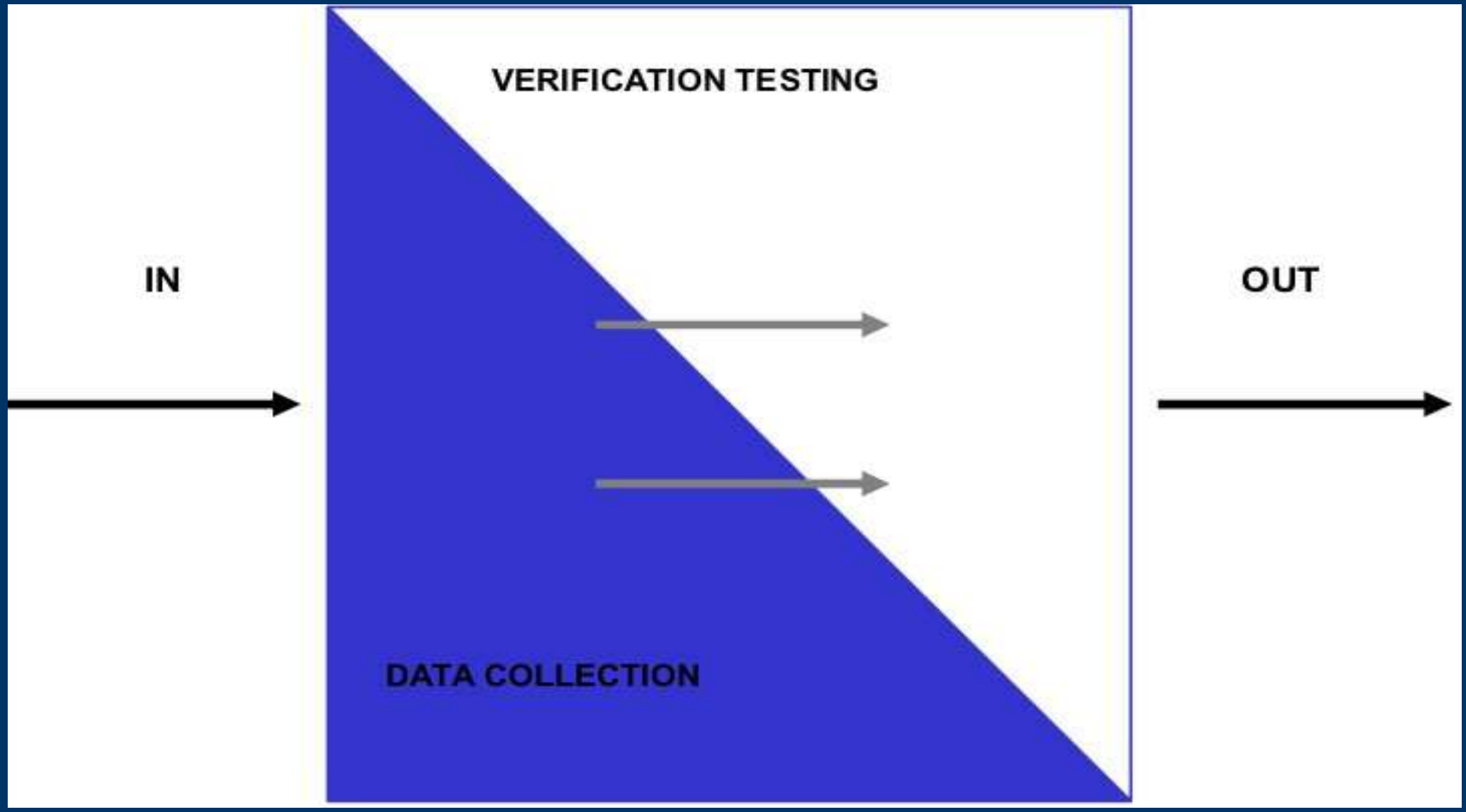
Módulos e tarefas

- Exemplo de um módulo



Metodologia

- Diagrama da metodologia



FIM!!!!

Eduardo Jorge Feres Serrano Neves - eth0
eduardo@securityopensource.org.br
serrano.neve@gmail.com.br