# Security Monitoring

Sarita Bora

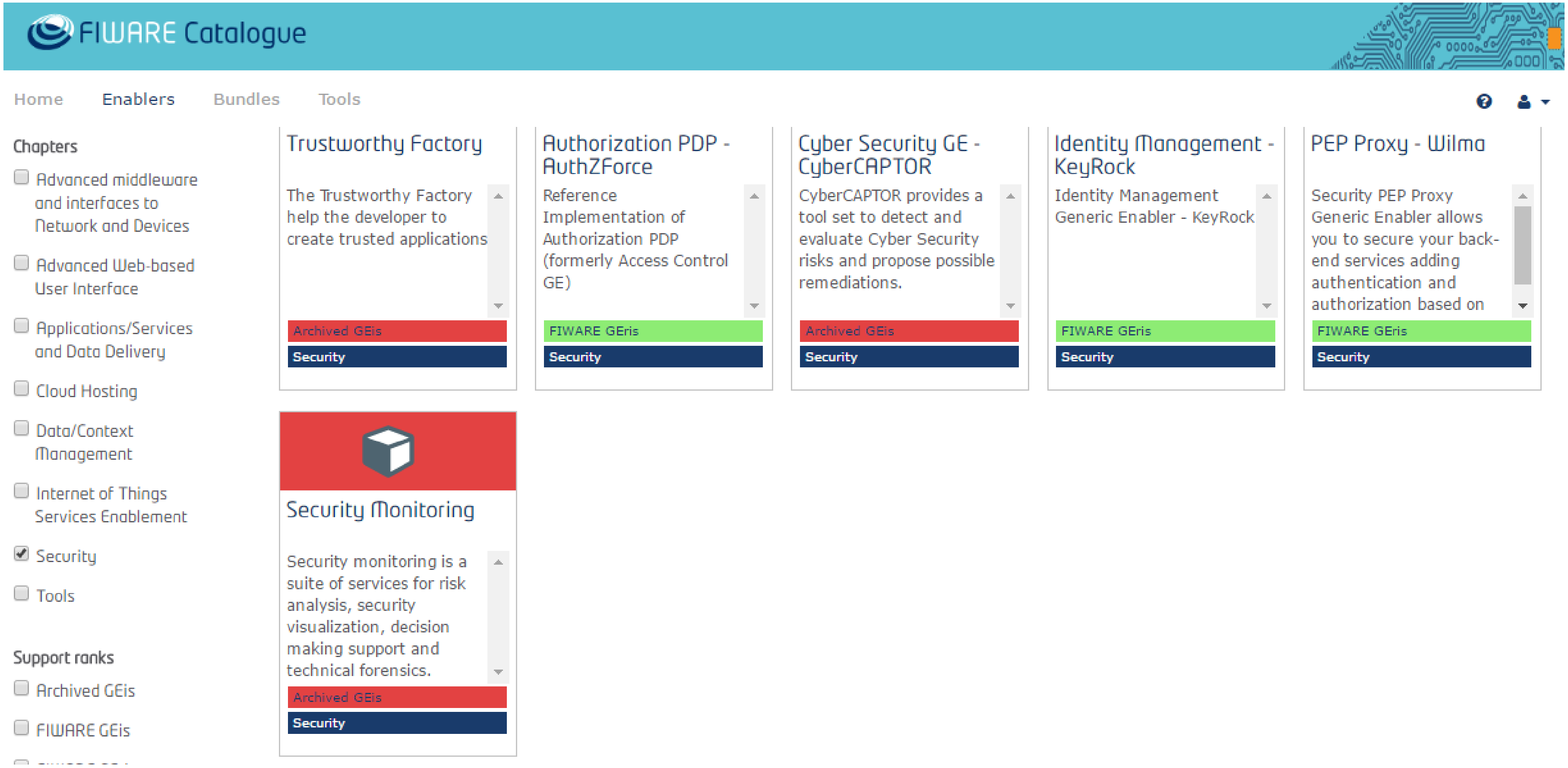
smb@cin.ufpe.br

# Agenda

- O que é?
- Principais funções
- Arquitetura
- Serviços oferecidos
- Demonstração

# O que é?

- Faz parte do sistema global de gerenciamento de segurança no FI-WARE e como tal faz parte de cada instância FI-WARE.
- É uma GE que lida não apenas com o monitoramento da segurança, mas com a proteção proativa de "ativos" em geral



FIWARE Catalogue

Home Enablers Bundles Tools

**Chapters**

- □ Advanced middleware and interfaces to Network and Devices
- □ Advanced Web-based User Interface
- □ Applications/Services and Data Delivery
- □ Cloud Hosting
- □ Data/Context Management
- □ Internet of Things Services Enablement
- ☑ Security
- □ Tools

**Support ranks**

- □ Archived GEis
- □ FIWARE GEis

**Trustworthy Factory**

The Trustworthy Factory help the developer to create trusted applications

Archived GEis

Security

**Authorization PDP - AuthZForce**

Reference Implementation of Authorization PDP (formerly Access Control GE)

FIWARE GEris

Security

**Cyber Security GE - CyberCAPTOR**

CyberCAPTOR provides a tool set to detect and evaluate Cyber Security risks and propose possible remediations.

Archived GEis

Security

**Identity Management - KeyRock**

Identity Management Generic Enabler - KeyRock

FIWARE GEris

Security

**PEP Proxy - Wilma**

Security PEP Proxy Generic Enabler allows you to secure your back-end services adding authentication and authorization based on

FIWARE GEris

Security

**Security Monitoring**

Security monitoring is a suite of services for risk analysis, security visualization, decision making support and technical forensics.

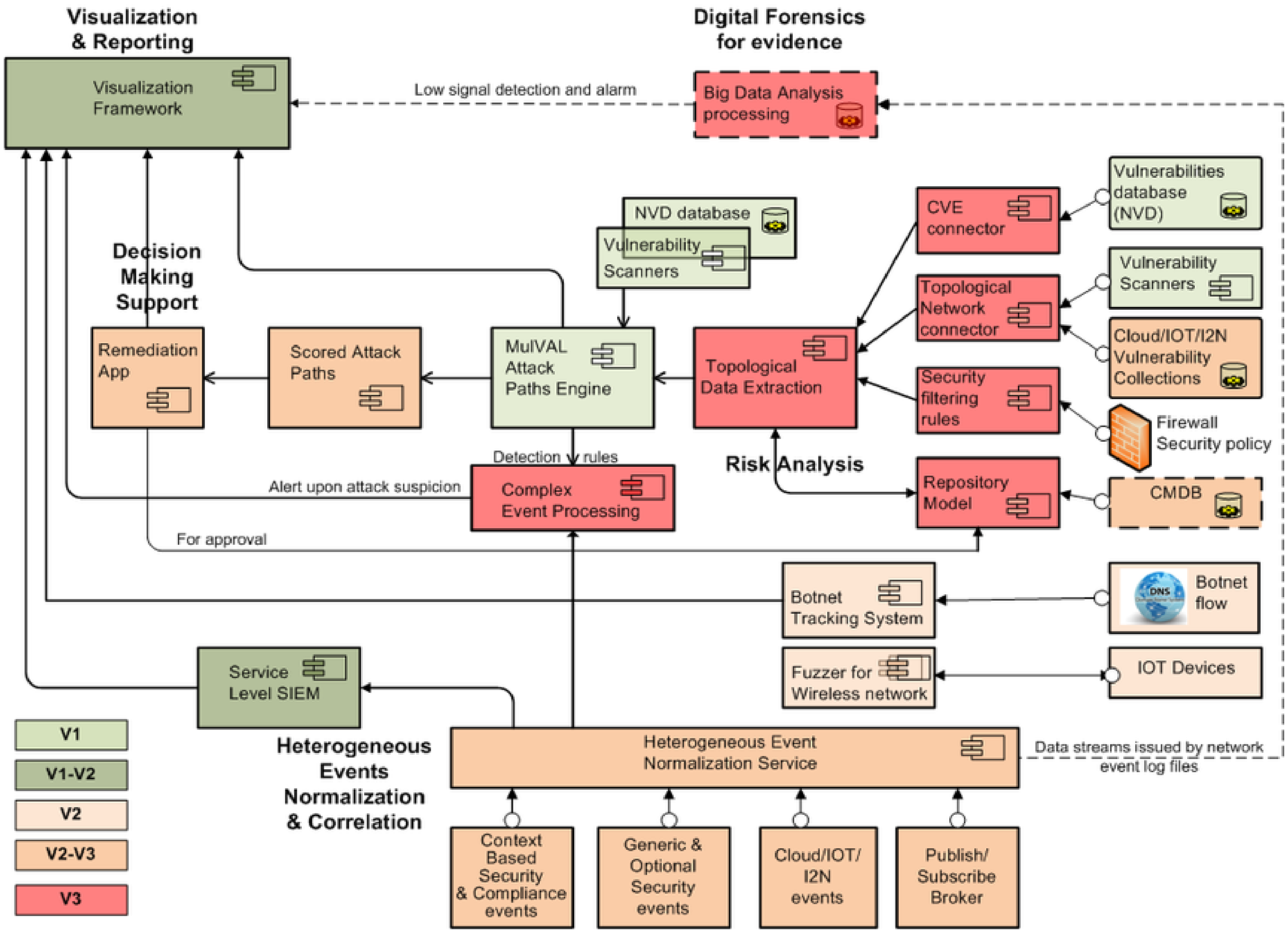
Archived GEis

Security

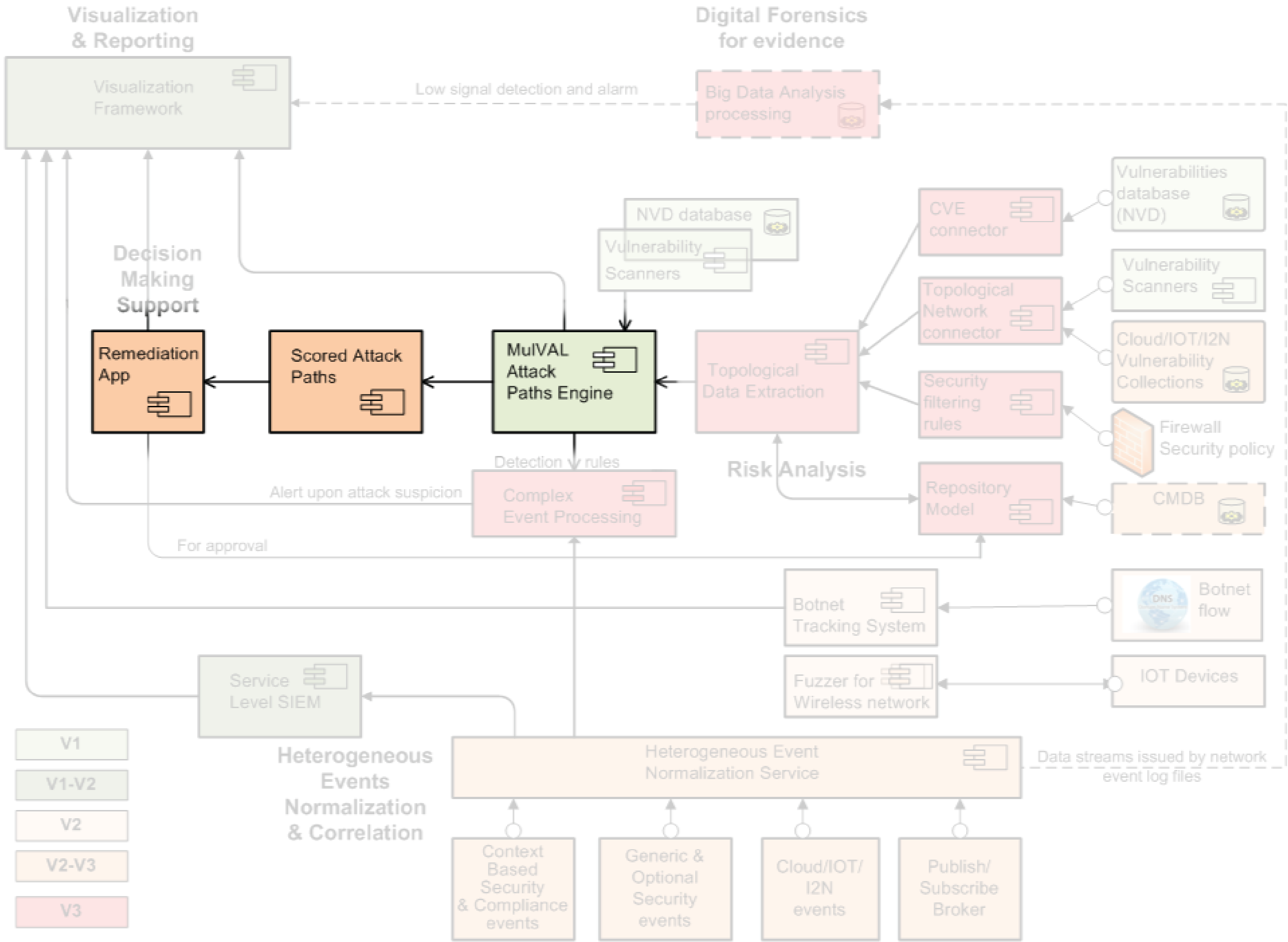
# Principais funções

- As principais funções desempenhadas pelo Security Monitoring são:
  - Normalizar e Correlacionar eventos, gerar alarmes
  - Identificar vulnerabilidades e avaliar potenciais ameaças
  - Mapear possíveis ataques e quantificar impactos sobre elementos essenciais
  - Avaliar riscos e propor soluções de remediação
  - Entregar um serviço de visualização de segurança orientada a usuário

# Arquitetura


Visualization & Reporting
Visualization Framework
Digital Forensics for evidence
Low signal detection and alarm
Big Data Analysis processing
Vulnerabilities database (NVD)
CVE connector
NVD database
Vulnerability Scanners
Decision Making Support
Vulnerability Scanners
Topological Network connector
Cloud/IOT/I2N Vulnerability Collections
Remediation App
Scored Attack Paths
MulVAL Attack Paths Engine
Topological Data Extraction
Security filtering rules
Firewall Security policy
Detection rules
Risk Analysis
Alert upon attack suspicion
Complex Event Processing
Repository Model
CMDB
For approval
Botnet Tracking System
Botnet flow
DNS
Service Level SIEM
Fuzzer for Wireless network
IOT Devices
V1
V1-V2
V2
V2-V3
V3
Heterogeneous Events Normalization & Correlation
Heterogeneous Event Normalization Service
Data streams issued by network event log files
Context Based Security & Compliance events
Generic & Optional Security events
Cloud/IOT/ I2N events
Publish/ Subscribe Broker

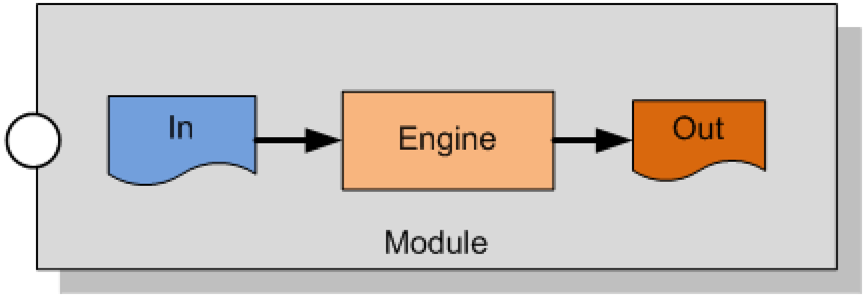
# Arquitetura


Visualization & Reporting
Visualization Framework
Low signal detection and alarm
Digital Forensics for evidence
Big Data Analysis processing
Vulnerabilities database (NVD)
CVE connector
NVD database
Vulnerability Scanners
Decision Making Support
Remediation App
Scored Attack Paths
MulVAL Attack Paths Engine
Topological Data Extraction
Topological Network connector
Vulnerability Scanners
Cloud/IOT/I2N Vulnerability Collections
Security filtering rules
Firewall Security policy
Detection rules
Risk Analysis
Alert upon attack suspicion
Complex Event Processing
Repository Model
CMDB
For approval
Botnet Tracking System
Botnet flow
DNS
Fuzzer for Wireless network
IOT Devices
Service Level SIEM
V1
V1-V2
V2
V2-V3
V3
Heterogeneous Events Normalization & Correlation
Heterogeneous Event Normalization Service
Data streams issued by network event log files
Context Based Security & Compliance events
Generic & Optional Security events
Cloud/IOT/ I2N events
Publish/ Subscribe Broker

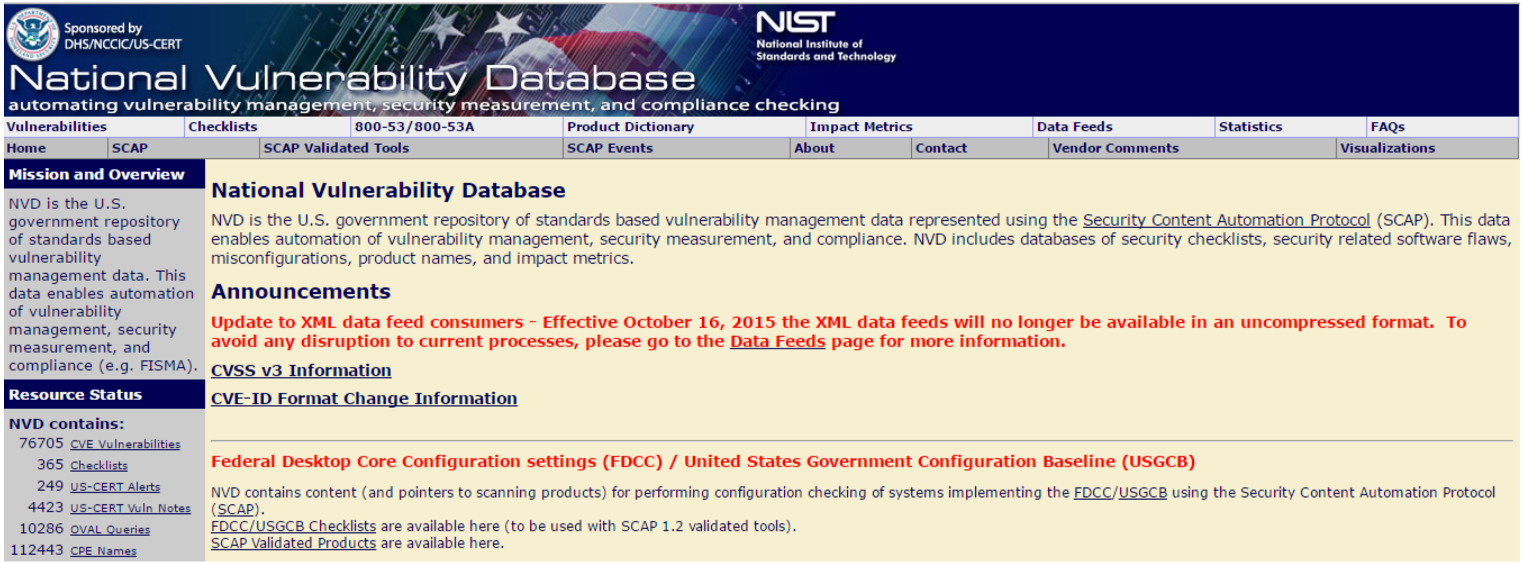
# Serviços

- Lista de serviços oferecido pelo Security Monitoring:
  - MulVAL Attack Paths Engine
  - Scored Attack Paths
  - Remediation

# MulVAL Attack Paths Engine



- O modelo utilizado na ferramenta de análise deve ser capaz de integrar automaticamente as especificações de vulnerabilidade formais a partir de fontes de vulnerabilidade heterogêneas.



National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

**Mission and Overview**

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

**Resource Status**

**NVD contains:**

| | |
|---|---|
| 76705 | CVE Vulnerabilities |
| 365 | Checklists |
| 249 | US-CERT Alerts |
| 4423 | US-CERT Vuln Notes |
| 10286 | OVAL Queries |
| 112443 | CPE Names |

## National Vulnerability Database

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

## Announcements

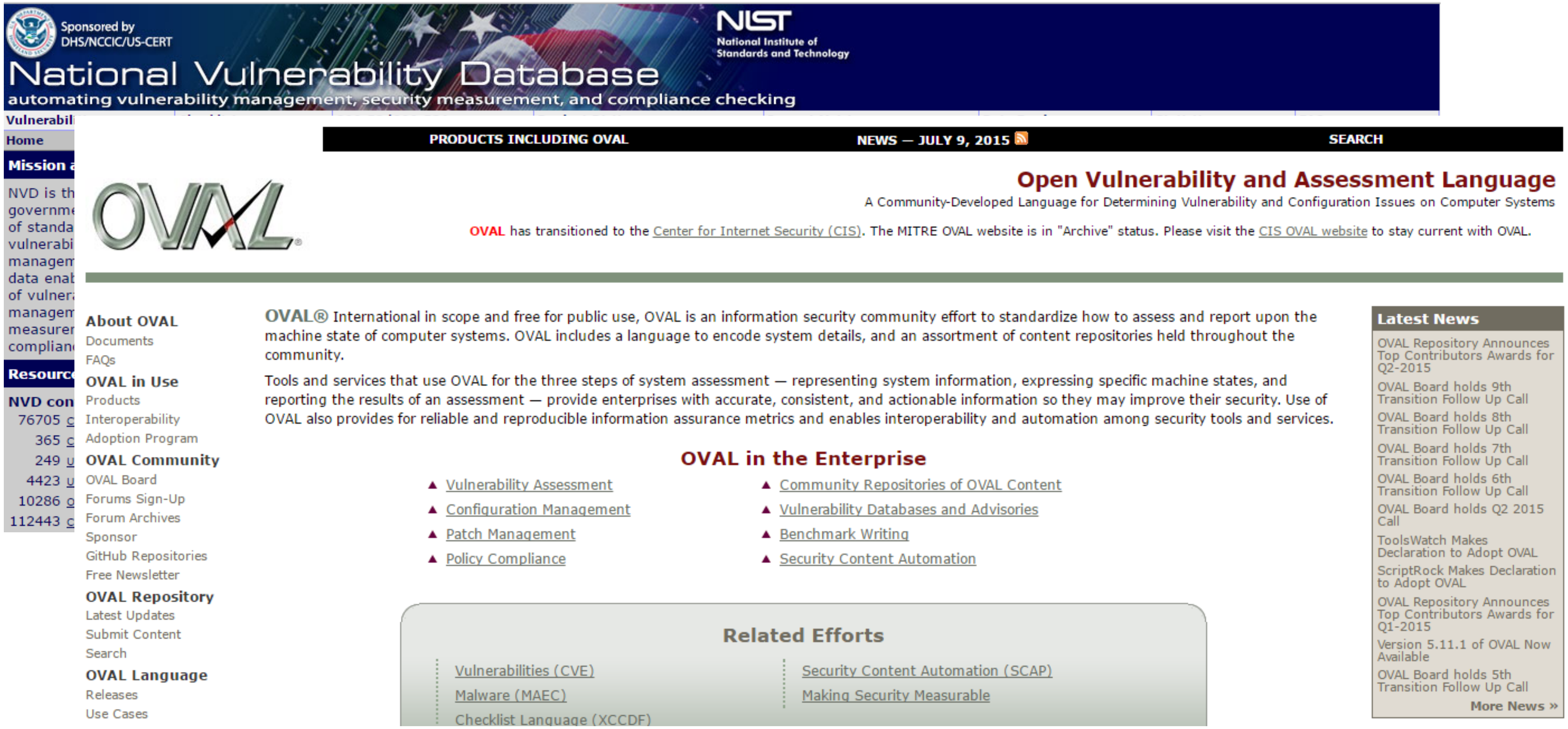
**Update to XML data feed consumers - Effective October 16, 2015 the XML data feeds will no longer be available in an uncompressed format. To avoid any disruption to current processes, please go to the Data Feeds page for more information.**

**CVSS v3 Information**

**CVE-ID Format Change Information**

**Federal Desktop Core Configuration settings (FDCC) / United States Government Configuration Baseline (USGCB)**

NVD contains content (and pointers to scanning products) for performing configuration checking of systems implementing the FDCC/USGCB using the Security Content Automation Protocol (SCAP).
FDCC/USGCB Checklists are available here (to be used with SCAP 1.2 validated tools).
SCAP Validated Products are available here.



Sponsored by DHS/NCCIC/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabil

Home

Mission a

NVD is th governm of standa vulnerabi managem data enat of vulnera managem measurem complian

Resourc

NVD con

76705 c

365 c

249 u

4423 u

10286 c

112443 c

## Open Vulnerability and Assessment Language

A Community-Developed Language for Determining Vulnerability and Configuration Issues on Computer Systems

OVAL has transitioned to the Center for Internet Security (CIS). The MITRE OVAL website is in "Archive" status. Please visit the CIS OVAL website to stay current with OVAL.

**About OVAL**
Documents
FAQs

**OVAL in Use**
Products
Interoperability
Adoption Program

**OVAL Community**
OVAL Board
Forums Sign-Up
Forum Archives
Sponsor
GitHub Repositories
Free Newsletter

**OVAL Repository**
Latest Updates
Submit Content
Search

**OVAL Language**
Releases
Use Cases

OVAL® International in scope and free for public use, OVAL is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security. Use of OVAL also provides for reliable and reproducible information assurance metrics and enables interoperability and automation among security tools and services.

### OVAL in the Enterprise

- Vulnerability Assessment
- Configuration Management
- Patch Management
- Policy Compliance
- Community Repositories of OVAL Content
- Vulnerability Databases and Advisories
- Benchmark Writing
- Security Content Automation

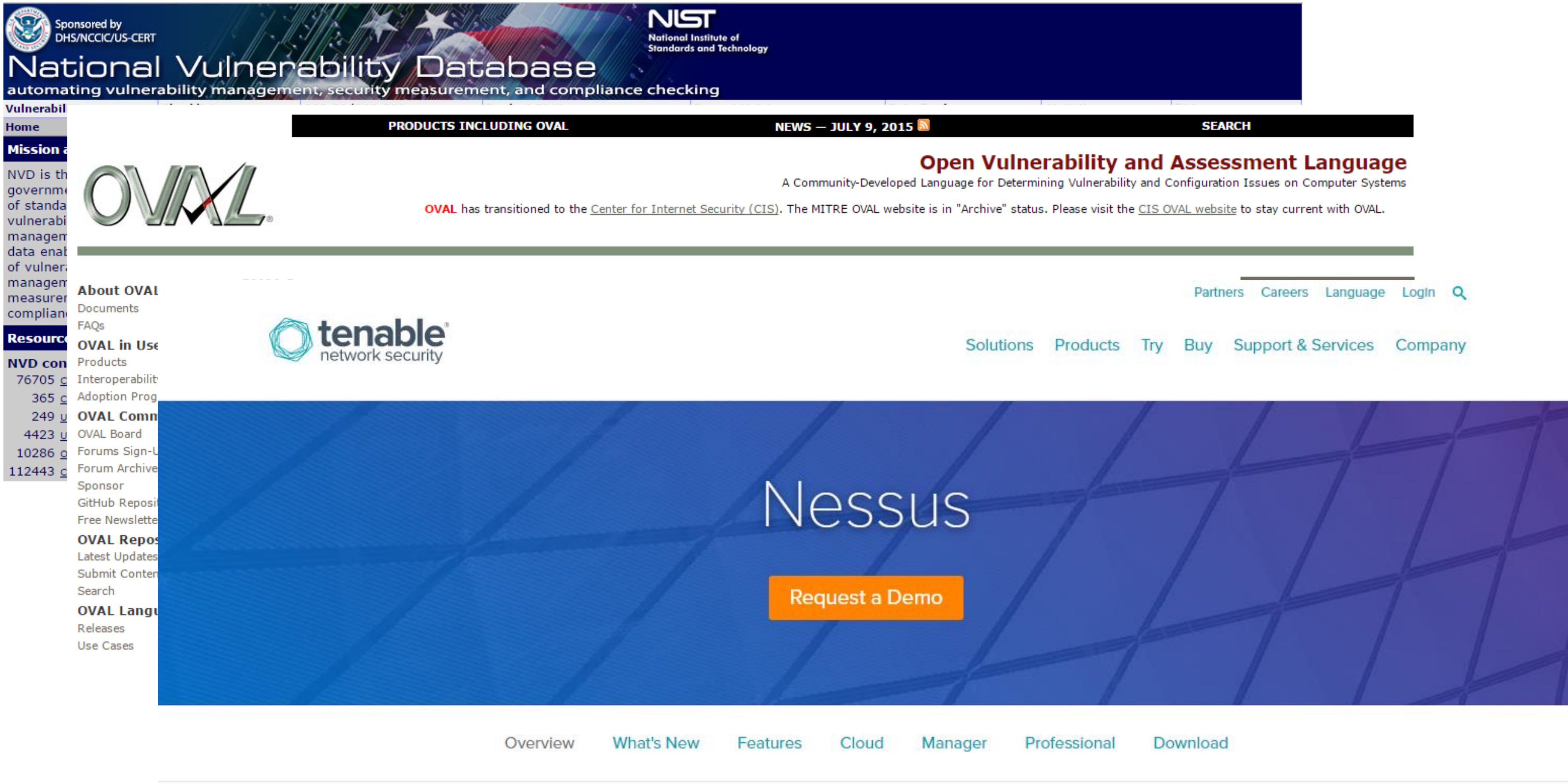
### Related Efforts

Vulnerabilities (CVE)
Malware (MAEC)
Checklist Language (XCCDF)
Security Content Automation (SCAP)
Making Security Measurable

**Latest News**

OVAL Repository Announces Top Contributors Awards for Q2-2015
OVAL Board holds 9th Transition Follow Up Call
OVAL Board holds 8th Transition Follow Up Call
OVAL Board holds 7th Transition Follow Up Call
OVAL Board holds 6th Transition Follow Up Call
OVAL Board holds Q2 2015 Call
ToolsWatch Makes Declaration to Adopt OVAL
ScriptRock Makes Declaration to Adopt OVAL
OVAL Repository Announces Top Contributors Awards for Q1-2015
Version 5.11.1 of OVAL Now Available
OVAL Board holds 5th Transition Follow Up Call

More News »



Sponsored by DHS/NCCIC/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabil

Home

Mission a

NVD is th governme of standa vulnerabi managem data enat of vulnera managem measurer complian

Resourc

NVD con

| | |
|---|---|
| 76705 | c |
| 365 | c |
| 249 | u |
| 4423 | u |
| 10286 | o |
| 112443 | c |

PRODUCTS INCLUDING OVAL NEWS — JULY 9, 2015 SEARCH

OVAL®

## Open Vulnerability and Assessment Language

A Community-Developed Language for Determining Vulnerability and Configuration Issues on Computer Systems

OVAL has transitioned to the Center for Internet Security (CIS). The MITRE OVAL website is in "Archive" status. Please visit the CIS OVAL website to stay current with OVAL.

About OVAL
Documents
FAQs
OVAL in Use
Products
Interoperabilit
Adoption Prog
OVAL Comn
OVAL Board
Forums Sign-U
Forum Archive
Sponsor
GitHub Reposi
Free Newslette
OVAL Repos
Latest Updates
Submit Conter
Search
OVAL Langu
Releases
Use Cases

Partners Careers Language Login

tenable network security

Solutions Products Try Buy Support & Services Company

Nessus

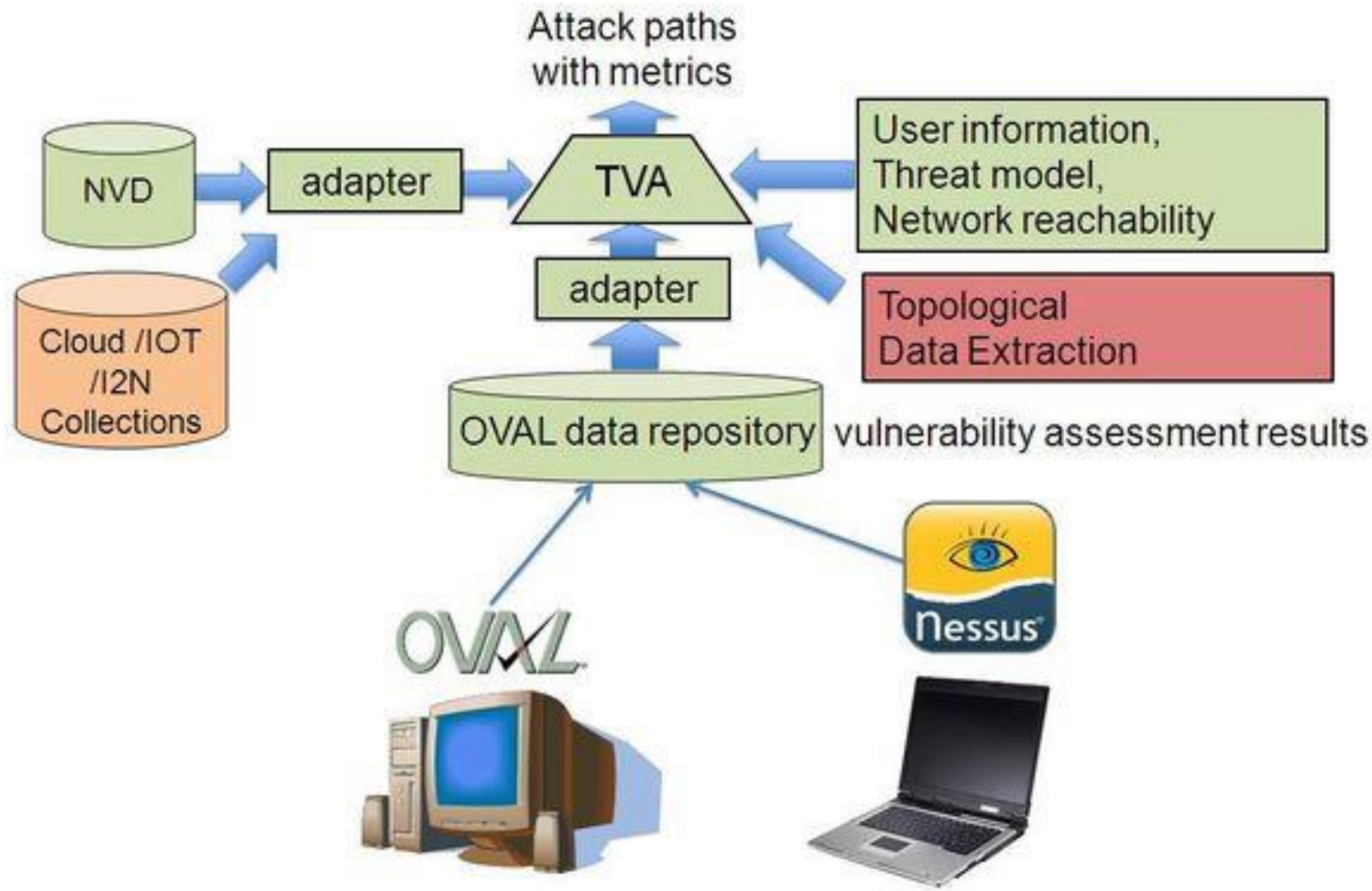
Request a Demo

Overview What's New Features Cloud Manager Professional Download

# MulVAL Attack Paths Engine

- É composto por quatro módulos:
  - Adaptadores
  - Core Attack Graph Computation
  - Análise de métricas;
  - Visualização do Attack Path;

# MulVAL Attack Paths Engine



Attack paths with metrics

NVD

adapter

TVA

User information, Threat model, Network reachability

Cloud /IOT /I2N Collections

adapter

Topological Data Extraction

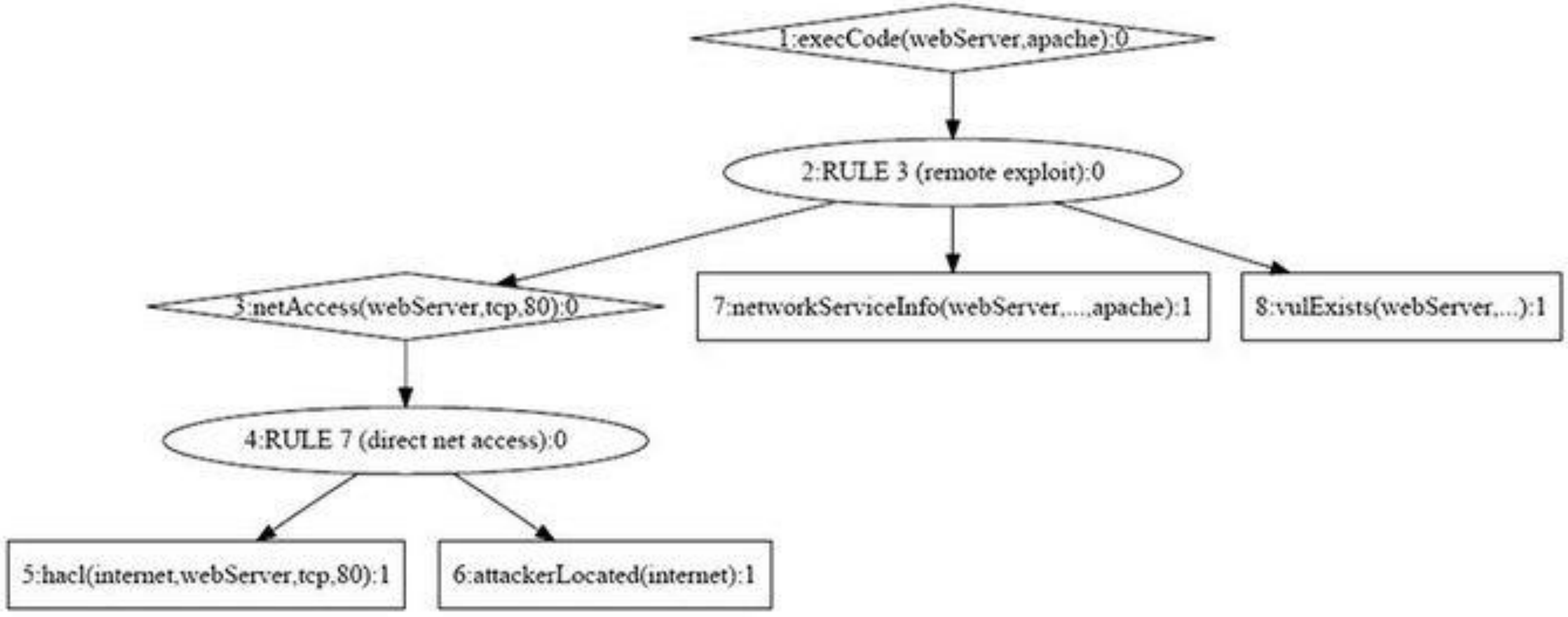
OVAL data repository

vulnerability assessment results

# MulVAL Attack Paths Engine

- Um caminho de ataque fornece o conjunto de hipóteses e operações que permitem ao atacante atingir um determinado alvo na infraestrutura de TI.
- Grafo de ataque fornece o conjunto completo de caminhos de ataque em potencial para essa infraestrutura, considerando simultaneamente todos os alvos combinados.

# MulVAL Attack Paths Engine


1:execCode(webServer,apache):0
2:RULE 3 (remote exploit):0
3:netAccess(webServer,tcp,80):0
7:networkServiceInfo(webServer,...,apache):1
8:vulExists(webServer,...):1
4:RULE 7 (direct net access):0
5:hacl(internet,webServer,tcp,80):1
6:attackerLocated(internet):1

Visualização do Attack Path/Graph

# Scored Attack Paths

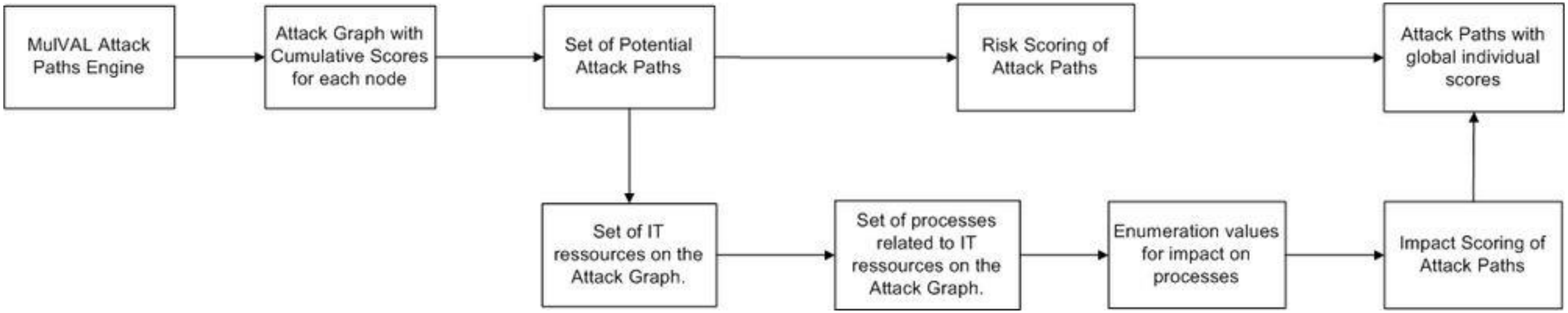
- Avalia o riscos e impactos dos caminhos de ataque;
- Interage com dois componentes: MulVAL Attack Paths Engine e Remediation

# Scored Attack Paths

É direcionado a usuários que desejam:

- Utilizar o serviço de Remediation
- Avaliar a situação de uma infra-estrutura de TI sob ponto de vista da segurança e impacto no negócio.
- Melhorar as configurações de segurança por meio de análises “what-if”

# Scored Attack Paths



MulVAL Attack Paths Engine

Attack Graph with Cumulative Scores for each node

Set of Potential Attack Paths

Risk Scoring of Attack Paths

Attack Paths with global individual scores

Set of IT ressources on the Attack Graph.

Set of processes related to IT ressources on the Attack Graph.

Enumeration values for impact on processes

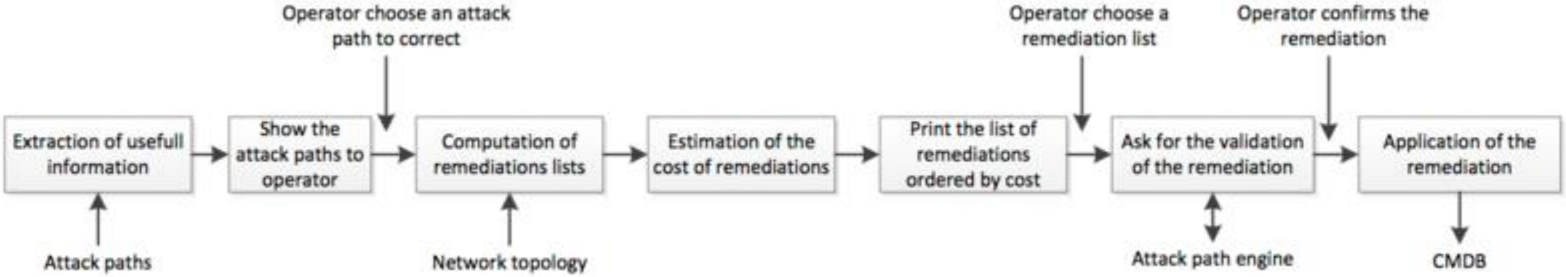
Impact Scoring of Attack Paths

# Remediation

É destinado a usuários que querem:

- Mostrar caminhos de ataque a um analista de segurança
- Ordenar caminhos de ataque por suas pontuações
- Aplicar uma função de custo para calcular um custo estimado de cada lista

# Remediation


Operator choose an attack path to correct
Operator choose a remediation list
Operator confirms the remediation
Extraction of usefull information
Show the attack paths to operator
Computation of remediations lists
Estimation of the cost of remediations
Print the list of remediations ordered by cost
Ask for the validation of the remediation
Application of the remediation
Attack paths
Network topology
Attack path engine
CMDB

# Demonstração

- MulVAL Attack Paths Engine Testbed Instance

  **Service Endpoint (URL):**http://secmonitoring.testbed.fi-ware.org/AttackGraphEngine/attackgraph.jsp

- Scored Attack Paths Testbed Instance

  **Service Endpoint (URL):**http://secmonitoring.testbed.fi-ware.org/ScoredAttackPaths

- Remediation Testbed Instance

  **Service Endpoint (URL):**http://secmonitoring.testbed.fi-ware.org/Remediation

# Referências

- http://catalogue.fiware.org/enablers/security-monitoring
- http://catalogue.fiware.org/enablers/security-monitoring/creating-instances
- https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.Security_Monitoring