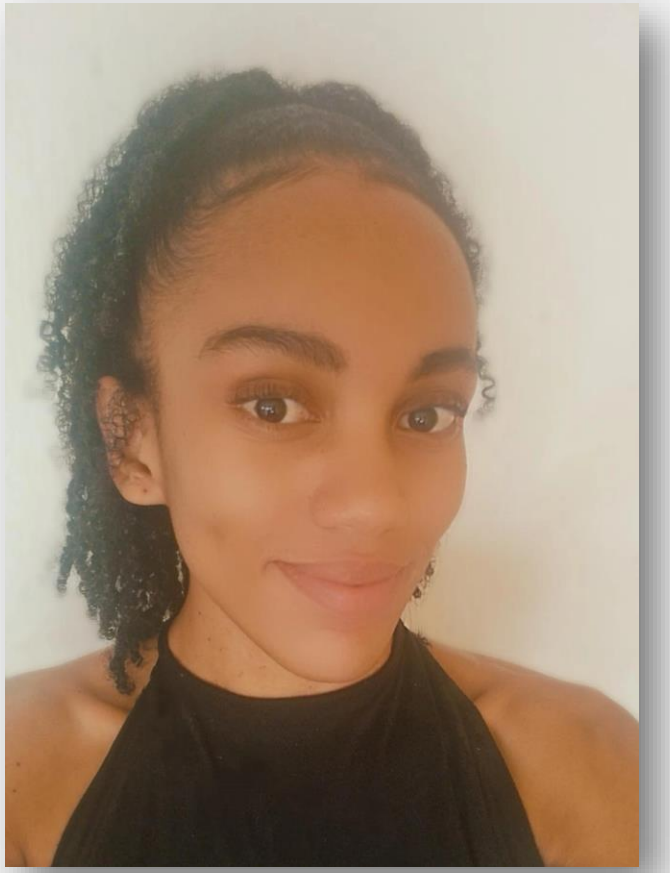
RNP Educação, Pesquisa e Inovação em Rede

Entendendo o gerenciamento de vulnerabilidades com o OpenVAS

Palestrante: Raquel Marques

Quem sou eu?



- ✓ Técnica em eletrônica - IFBA (Campus Salvador-BA)
- ✓ Graduanda em Ciência da Computação (UFBA)
- ✓ Membra do Programa Onda Digital (POD-UFBA)
- ✓ Membra do Projeto Meninas Digitais Regional Bahia (MD-BA)
- ✓ Participante do Programa de Mentoria de IT Women 2023 - "Identificação de padrões de fraudes disseminadas via redes sociais" (LACNIC)
- ✓ Integrante da equipe de segurança da informação do PoP-BA/RNP

Agenda

- ✓ A importância do scanner de vulnerabilidade na sua organização
- ✓ Apresentação do OpenVAS GVM
- ✓ Produtos de gerenciamento de vulnerabilidades da Greenbone
- ✓ Greenbone Community Edition 22.04
- ✓ Vantagens e Desvantagens do Greenbone commutity Edition 22.04

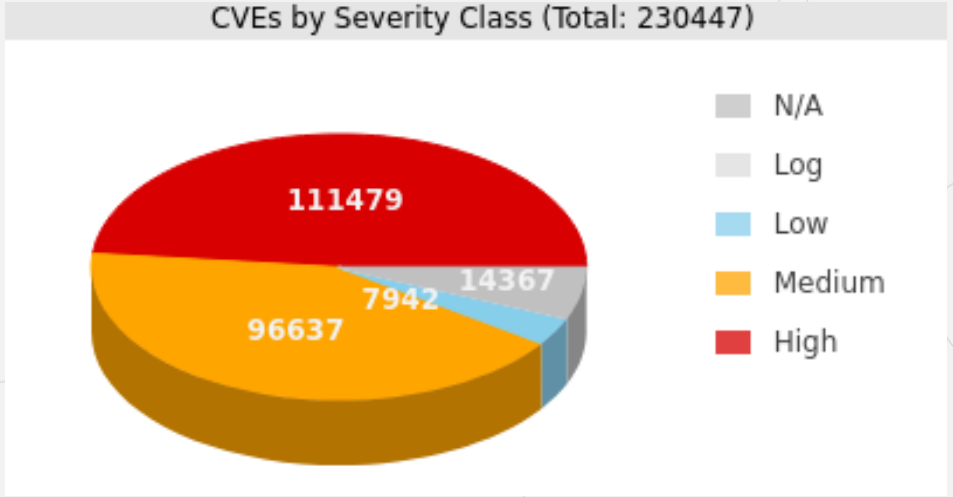
RNP

Educação, Pesquisa
e Inovação em Rede

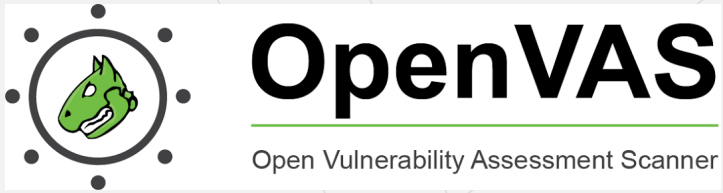
A importância do scanner de vulnerabilidade na sua organização

Vulnerabilidades Identificadas pelo OpenVAS

Novas vulnerabilidades estão sempre surgindo, sendo assim, o processo de identificação e correção das falhas de segurança em dispositivos, redes e aplicações precisa ser contínuo para reduzir o risco e o impacto dos ataques cibernéticos.



A Função do Scanner de Vulnerabilidades



Um scanner de vulnerabilidades é um software usado para identificar e reportar as vulnerabilidades de um determinado alvo. A avaliação de vulnerabilidade produzida pelo scanner de vulnerabilidade é usada para implementar ações corretivas para as vulnerabilidades identificadas, tornando o sistema mais seguro.

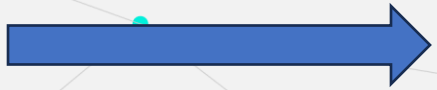
RNP

Educação, Pesquisa
e Inovação em Rede

Apresentação do OpenVAS GVM

OpenVAS GVM

O OpenVAS é um scanner de vulnerabilidade completo, o qual vai além de uma simples varredura de vulnerabilidades. Ele oferece recursos que auxiliam no gerenciamento das vulnerabilidades.



OpenVAS GVM

O OpenVAS foi desenvolvido com base nos seguintes propósitos:

- Ir além da verificação rigorosa da vulnerabilidade em direção a uma análise abrangente para a solução de gerenciamento de vulnerabilidades.
- Criação de um produto/aparelho para clientes corporativos.
- Continuar o conceito de código aberto, com o intuito de criar uma tecnologia transparente de segurança da informação.

RNP

Educação, Pesquisa
e Inovação em Rede

Produtos de gerenciamento de vulnerabilidades da Greenbone

Greenbone Vulnerability Management

Fig. 3.1 Greenbone Enterprise Appliance for large organizations

Comercial

- Dispositivos de hardware
- Dispositivos virtuais
- Serviço de nuvem da Greenbone

Community

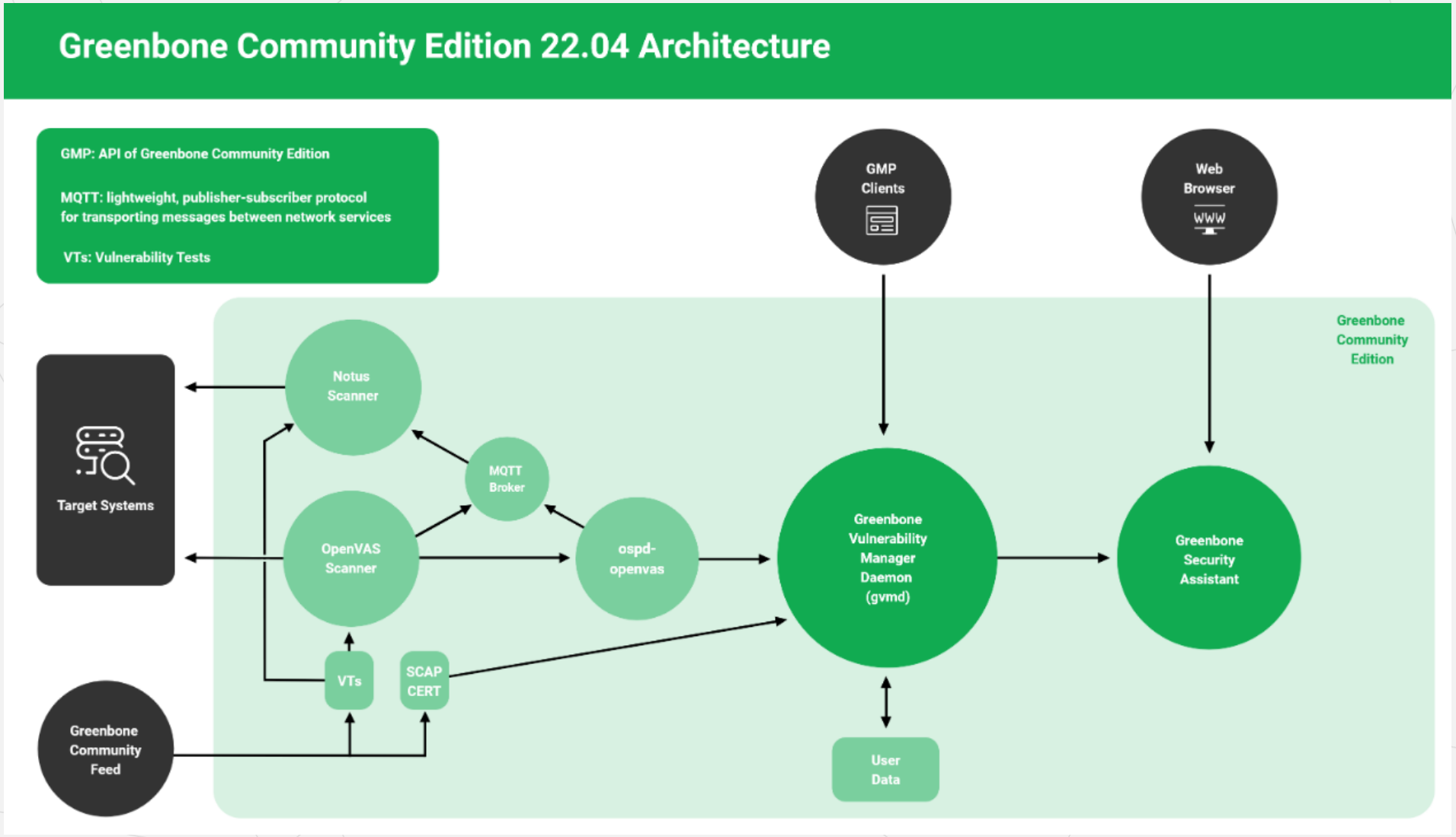
- Greenbone Community Edition 22.04

RNP

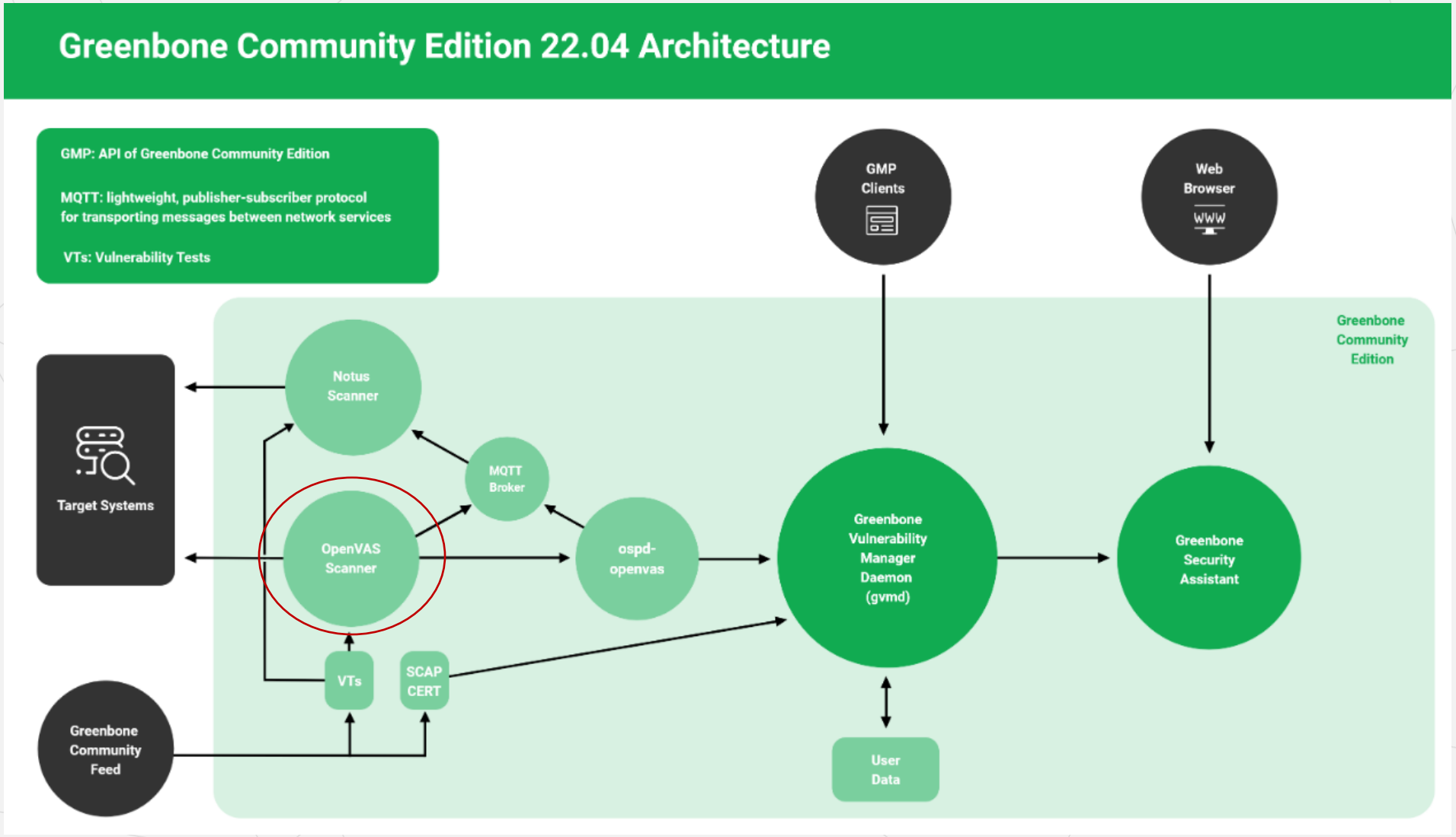
Educação, Pesquisa
e Inovação em Rede

Greenbone Community Edition 22.04

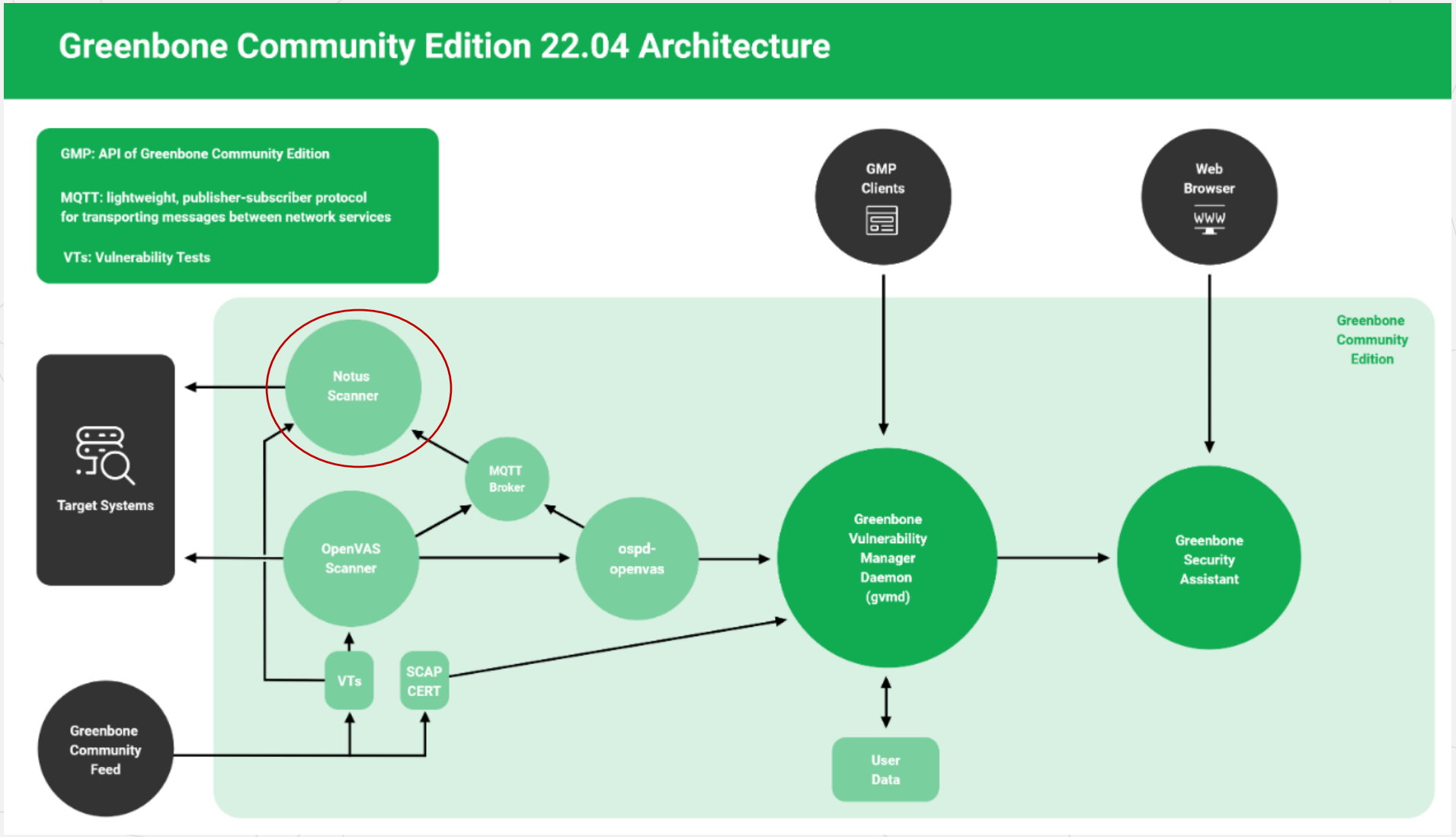
Apresentação da Arquitetura



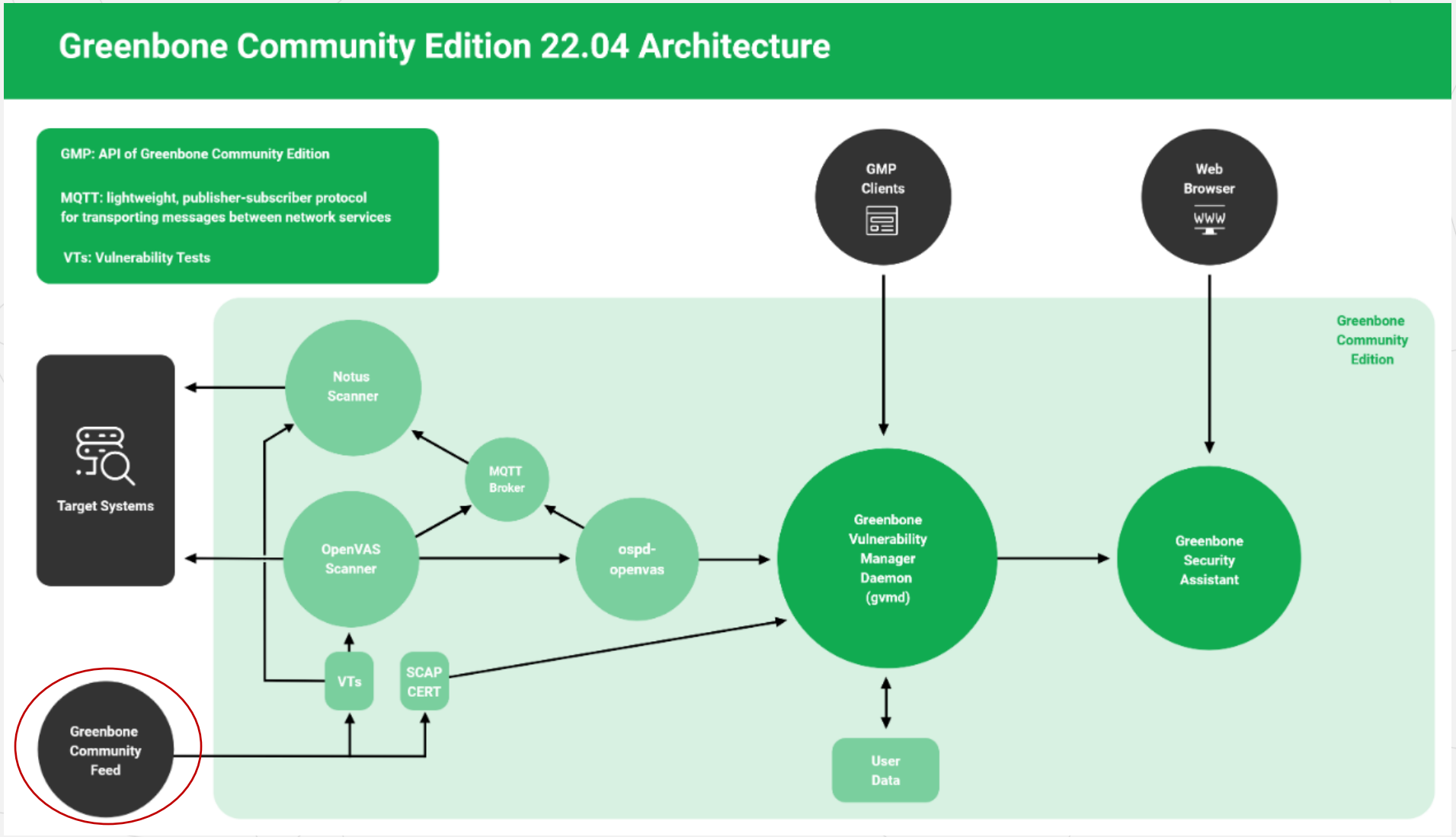
Apresentação da Arquitetura – OpenVAS Scanner



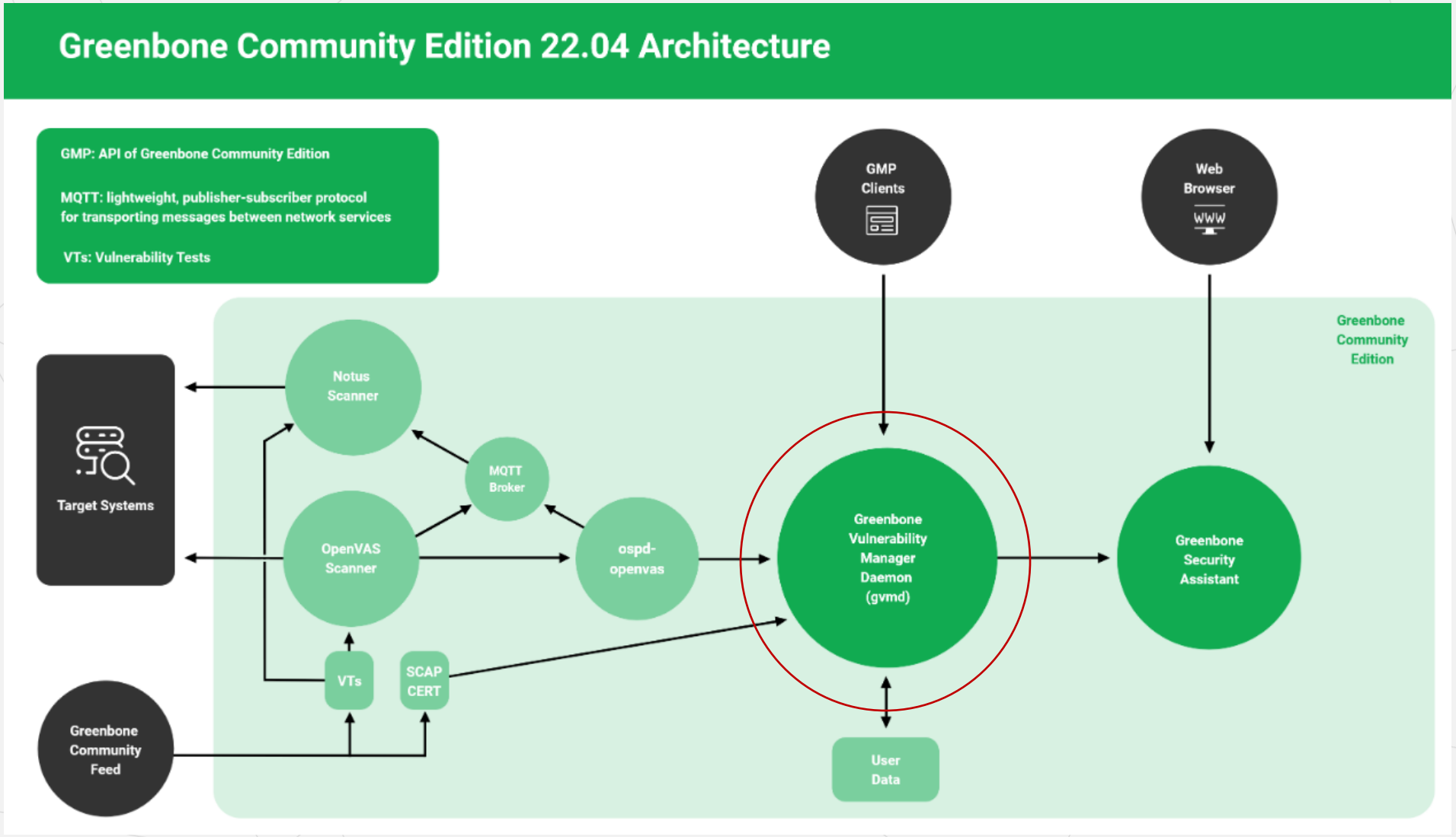
Apresentação da Arquitetura – Notus Scanner



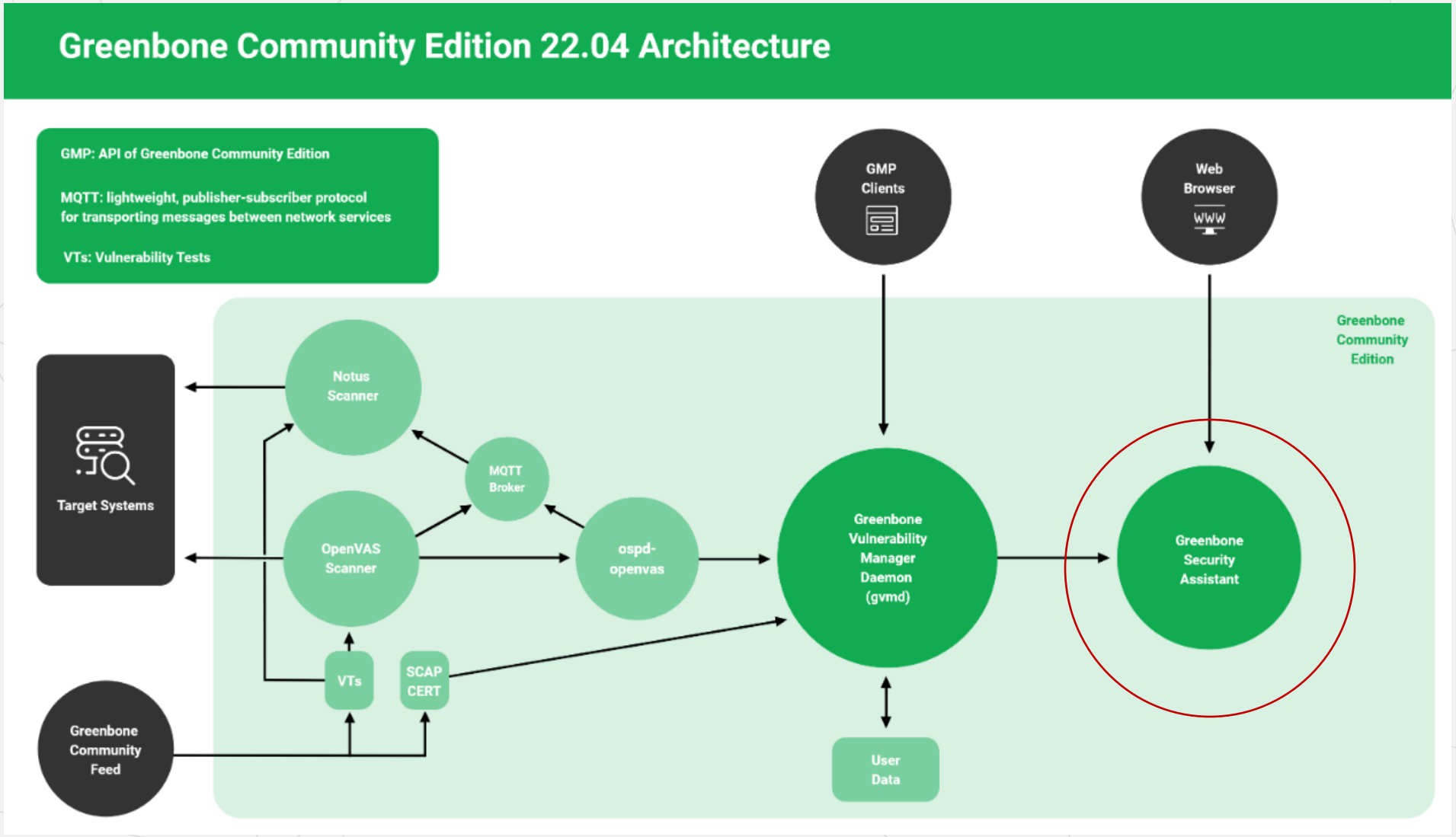
Apresentação da Arquitetura – Greenbone Community Feed



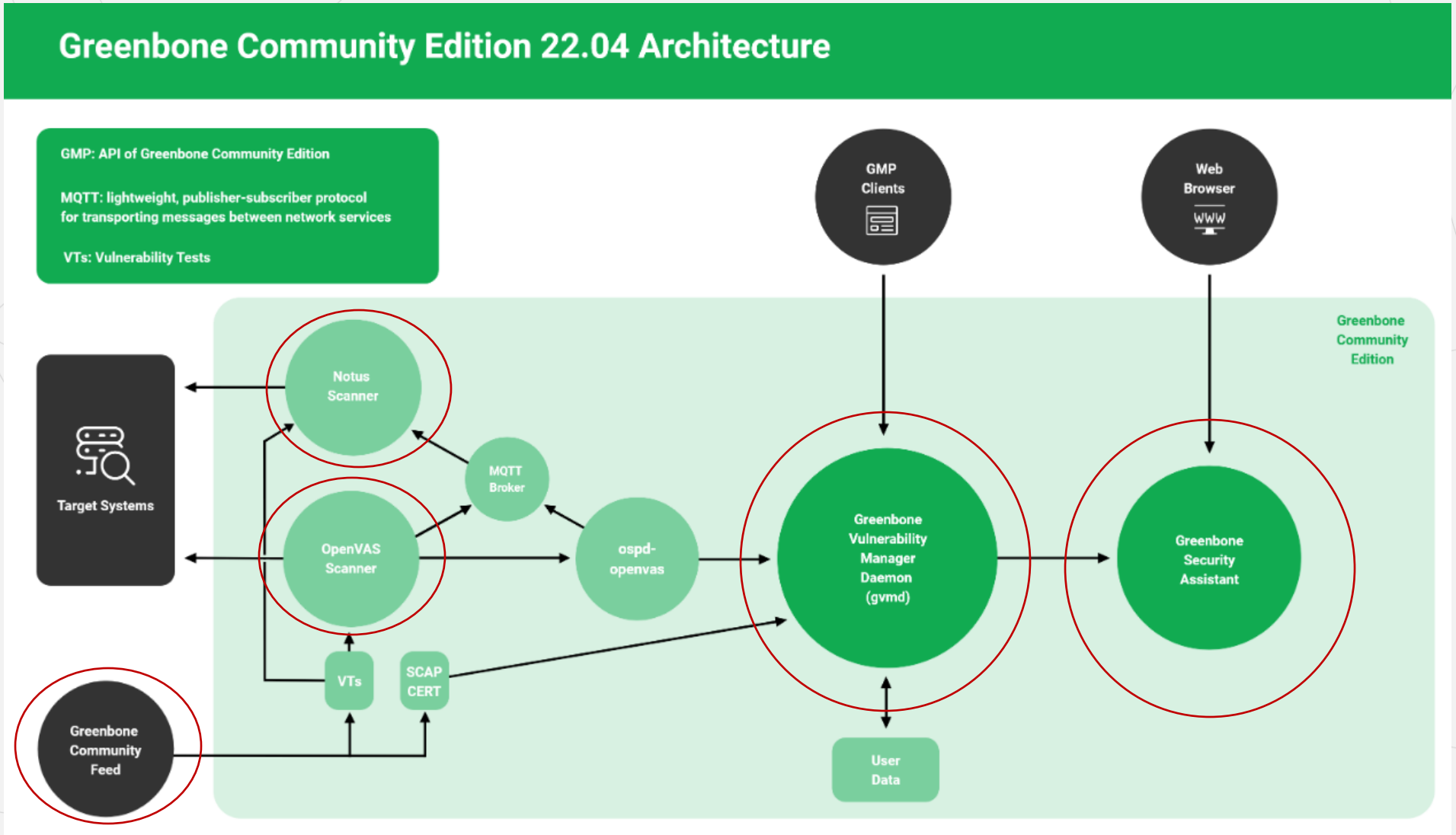
Apresentação da Arquitetura - GVMD



Apresentação da Arquitetura - GSA



Apresentação da Arquitetura



Processo de Instalação

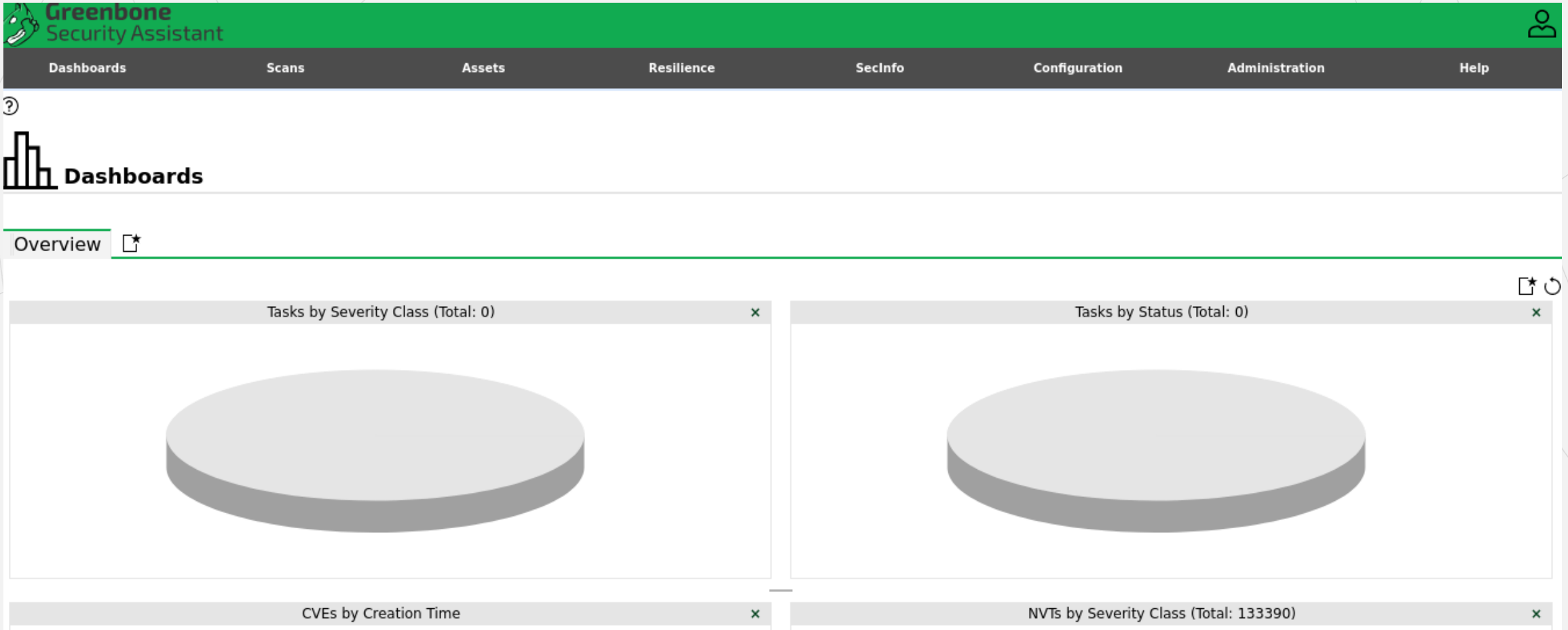
- Podemos instalar através do código-fonte ou dos containers.
- É disponibilizado para as seguintes distribuições:
  - Debian estável,
  - Ubuntu 22.04 LTS,
  - Fedora 35 e 36
  - CentOS 9
- Site: https://greenbone.github.io/docs/latest/background.html

Nota

Esteja ciente dos seguintes efeitos colaterais gerais:

- Mensagens de log e alerta podem aparecer nos sistemas de destino.
- Mensagens de registro e alerta podem aparecer em dispositivos de rede, soluções de monitoramento, firewalls e sistemas de detecção e prevenção de intrusões.
- Regras de firewall e outras medidas de prevenção de intrusões podem ser acionadas.
- As verificações podem aumentar a latência no destino e / ou na rede digitalizada. Em casos extremos, isso pode resultar em situações semelhantes a um ataque de negação de serviço (DoS).
- As verificações podem desencadear bugs em aplicativos frágeis ou inseguros, resultando em falhas ou falhas.
- Sistemas embarcados e elementos de tecnologia operacional com pilhas de rede fracas estão especialmente sujeitos a possíveis falhas ou mesmo dispositivos quebrados.
- Os logins (por exemplo, via SSH ou FTP) são feitos contra os sistemas de destino para fins de captura de banner.
- As verificações podem resultar no bloqueio de contas de usuário devido ao teste de combinações padrão de nome de usuário / senha.

Interface Web do Usuário



Interface Web do Usuário

- Criação de tarefas personalizadas;
- Visualização dos resultados do scan;
- Configuração de usuários, grupos e permissões de acesso.
- Criação de alerta.
- Geração de relatórios.

Classificação da Severidade das Vulnerabilidades

CVSSv2 Base Score Calculator

From Metrics:

Access Vector	Local
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity	None
Availability	None

From Vector:

Vector	AV:L/AC:L/Au:N/C:N/I:N/A:N

Results:

CVSS Base Vector	AV:L/AC:L/Au:N/C:N/I:N/A:N
Severity	0.0 (Log)

CVSSv3 Base Score Calculator

From Metrics:

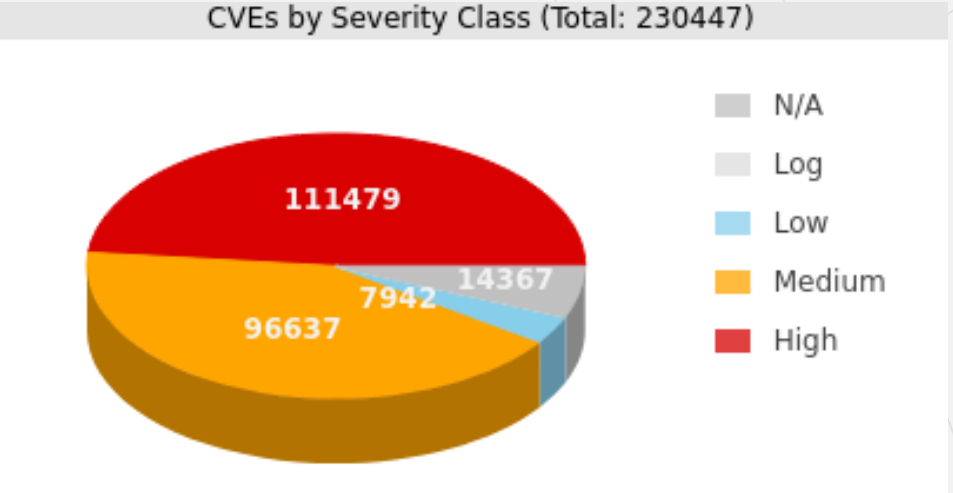
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	None

From Vector:

CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/U

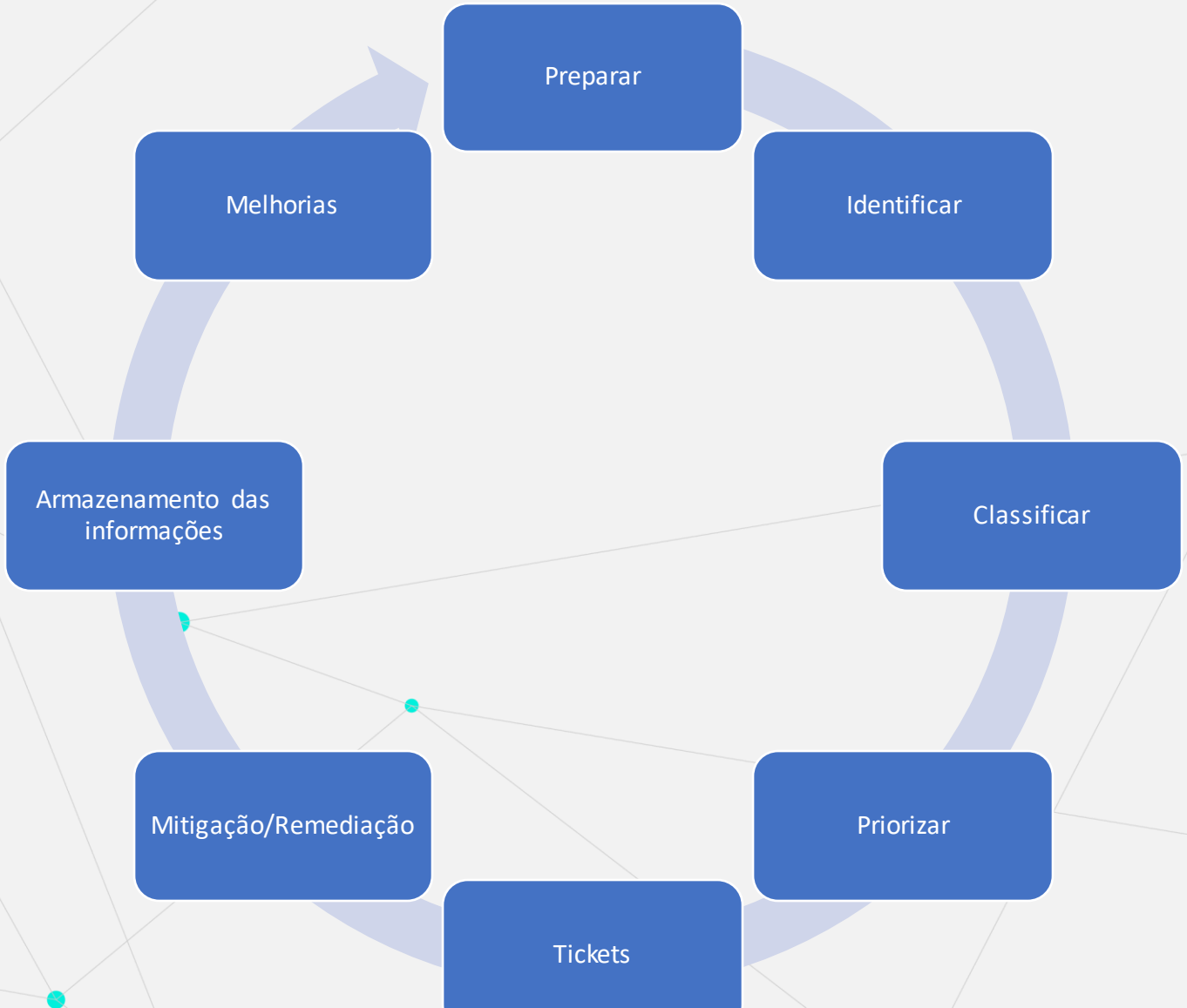
Results:

CVSS Base Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Severity	0.0 (Log)



Site: www.first.org/cvss/

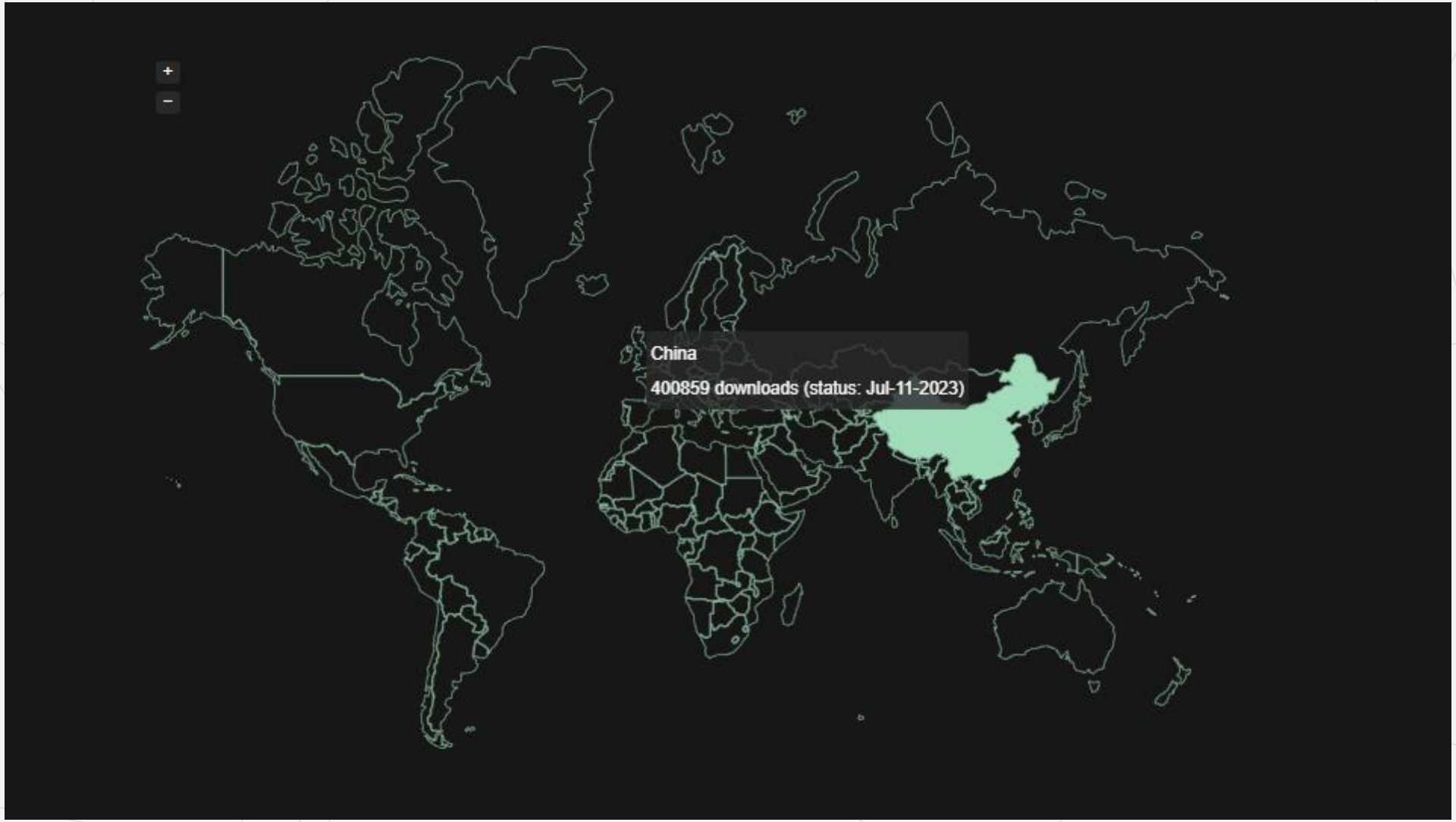
Ciclo do OpenVAS GVM



Downloads da versão community pelo mundo

Downloads da versão community pelo mundo

Downloads da versão community pelo mundo



Downloads da versão community pelo mundo

RNP

Educação, Pesquisa
e Inovação em Rede

Vantagens e Desvantagens do Greenbone Community Edition 22.04

Considerações Finais

Vantagens

- Scanner de vulnerabilidades completo.
- Comunidade ativa.
- Melhorias constantes do serviço

Desvantagens

- Processo de instalação

Dúvidas?

OBRIGADA!

openvas.org

greenbone.net

raquel.marques@pop-ba.rnp.br