17º WRNP Workshop RNP

30 | 31 MAIO
SALVADOR | BA

PILOTO

GT-EWS: Mecanismos para um sistema de alerta antecipado

EQUIPE

Coordenadores
Daniel Macêdo Batista (IME/USP)
Luiz Arthur F. Santos (UTFPR-CM)
Rodrigo Campiolo (UTFPR-CM)

Gerente de projeto
Wagner A. Monteverde (UTFPR-CM)

Desenvolvedores
Éder dos S. Ferreira (UTFPR-CM)
Marlon F. Antônio (UTFPR-CM)
Thiago L. Vieira (UFSCar)

Parceiros
Centro de Atendimento a Incidentes de Segurança da RNP (CAIS)
Universidade de São Paulo (USP)
Universidade Tecnológica Federal do Paraná (UTFPR)
Polícia Federal
Universidade Federal da Bahia (UFBA)
Processamento de Dados do Amazonas (Prodam)

SITE

http://gtews.ime.usp.br/

CONTATO

Gerência de Grupos de Trabalho da RNP
ggt@rnp.br

DESCRIÇÃO

A proposta de piloto do EWS é um sistema capaz de detectar antecipadamente a orquestração de ataques, vazamento de dados, desfigurações de páginas *web* e vulnerabilidades de sistemas ou aplicativos no escopo da RNP.

A arquitetura do EWS contempla um ou mais sensores; módulos acopláveis de pré-processamento; um núcleo de processamento centralizado; e uma interface *web* (Figura 1). O piloto está disponível em https://horus.rnp.br.

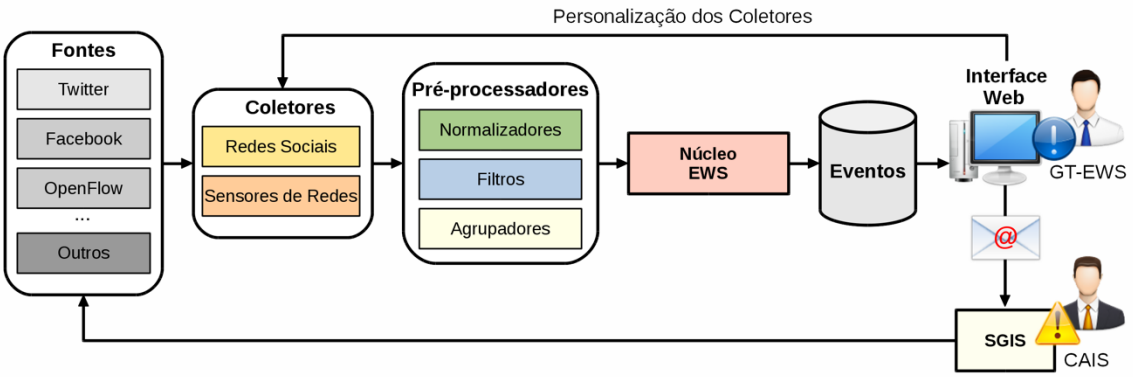

Figura 1: Arquitetura do EWS.

DEMONSTRAÇÕES

Demonstração 1: Detecção de tentativa de ataque por meio da orquestração desse ataque no Twitter e Facebook.

Figura 2: Monitoramento de orquestração de ataque.

Demonstração 2: Detecção e registro de desfiguração de páginas (*defacement*) anunciada em redes sociais.

Figura 3: Monitoramento e registro de desfiguração de página.

Demonstração 3: Configuração e acoplamento de novos sensores.

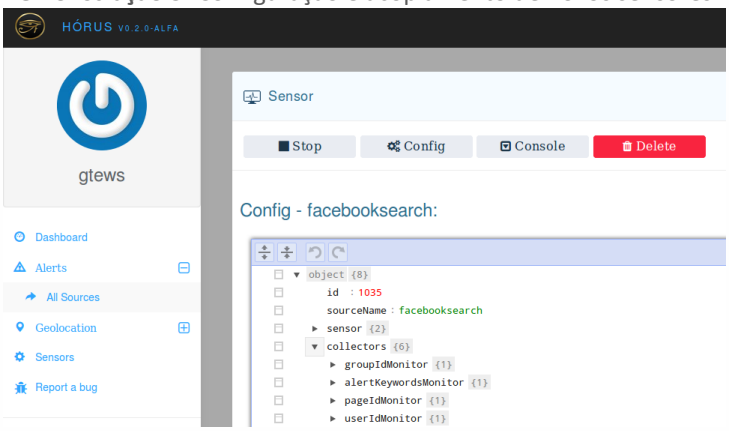

Figura 4: Configuração de sensor remoto.