

Sistema imunológico artificial aplicado para detecção de intrusão (SIA-DI)

BR 51 2016 000190 9

Autor(es): João Bosco Mangueira Sobral, Lucas Marcus Bondnar e Renato Bobsin Machado.

Titular(es): UNIOESTE/UFSC

Patente Nacional: INPI

Data de Protocolo: 26/02/2016

Data de Publicação: 29/03/2016 **RPI:** 2360

Descrição:

O Sistema Imunológico Artificial aplicado para Detecção de Intrusão (SIA-DI) consiste em uma solução computacional bioinspirada para a detecção de intrusão em servidores de rede de computadores, de modo distribuído. Como principais características, o SIA-DI é em um sistema de detecção de intrusão baseado em anomalias, com arquitetura centralizada, baseada em host e gerando respostas passivas (por meio do envio de emails aos administradores) e ativas por meio do isolamento do(s) serviço(s) atacados. Para a geração de eventos foram utilizados os geradores de logs Syslog e Syslog-ng, e para a tarefa de análise foi aplicada a ferramenta Logcheck por meio de uma base de dados adaptada pelo SIA-DI.