18º WRNP
Workshop RNP
15 | 16 MAIO
Belém | PA

GT-BIS
Mecanismos para Análise de Big Data em Segurança da Informação

Daniel Macêdo Batista (USP) batista@ime.usp.br

Problema

- Aumento nas taxas de transmissão da Internet
  - Maior interesse de atacantes
  - Necessidade de monitoramento em mais pontos da rede, mas com taxas de amostragem
    - **765.000 pacotes** por segundo, **16.371 eventos** por segundo, **1,3TB** por dia
  - Ataques podem não ser detectados
- Difícil de ter o sistema ideal
  - Monitoramento apenas em momentos relevantes
  - Armazenamento do mínimo de dados para detecção em memória volátil
  - Armazenamento do mínimo de dados para investigações e aprendizado automático na memória não volátil
- Usar ferramentas para análise de big data pode ser útil na correlação de eventos e detecção antecipada de ataques
  - Processamento de fluxo em tempo real
  - Armazenamento seletivo de dados
  - Aprendizado profundo
  - Aprendizado de máquina (Qual a melhor técnica? Como escalar?)

Objetivos

- Arquitetura para análise de big data de sensores distribuídos heterogêneos, em busca de ataques o mais rápido possível
- Análise de desempenho, e de falsos positivos e falsos negativos, em busca da melhor técnica de correlação de dados que antecipe ataques
- Mecanismo de aprendizado de ataques simples (protótipo para um mecanismo mais robusto para ataques compostos por diversas etapas)
- Interface web para configuração do sistema e visualização dos resultados das análises

Solução preliminar