Detecção de ataques utilizando a IA

Conjuntos de informações relevantes para a área de cibersegurança

Feito por: Davi J L Santos

SUMARIO

1

Introdução

Atualmente, o tráfego de informações nas redes está em constante crescimento, podendo atingir até 20 tbit/s, conforme relatado pelo IX.BR em 06/12/2021.

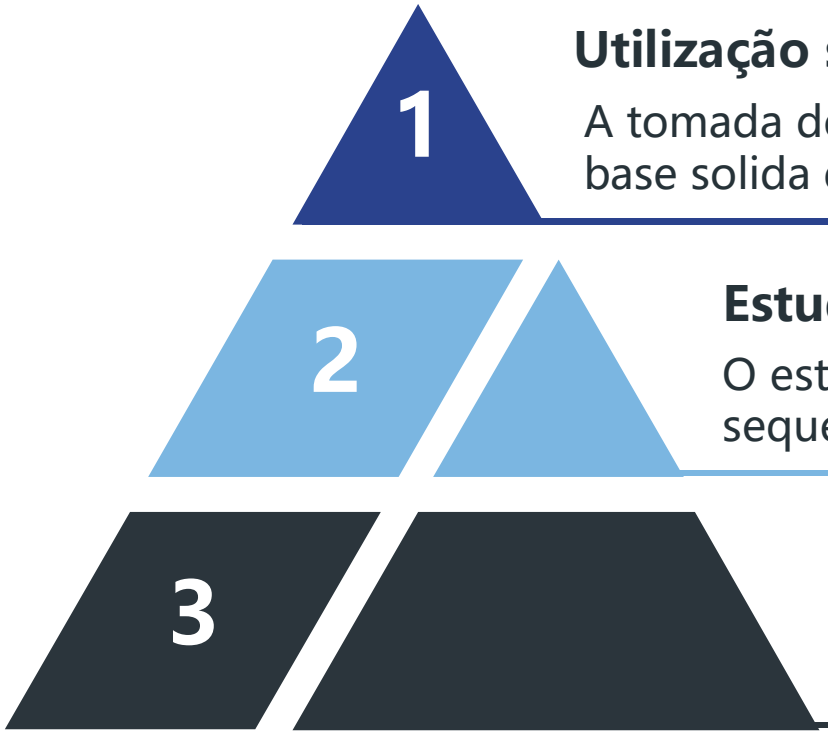
Esse aumento no tráfego também vem acompanhado de um crescente número de ataques cibernéticos, o que gera uma grande quantidade de informações a serem analisadas e tratadas.

INTRODUÇÃO

Identificar essas atividas maliciosas em redes e sistemas por base em comportamentos anômalos

O QUE FAZER?

INTRODUÇÃO



Utilização sem baseada

A tomada de decisão deve ser sempre baseada em uma base solida de informações.

Estudo de Corsini et al. (2021):

O estudo avalia técnicas de aprendizado de máquina sequencial para a detecção de ataques cibernéticos.

Estudo de Das e Sandhane (2021):

Ele explora o uso da inteligência artificial na segurança cibernética para a detecção de intrusões.

Utilizar os meios para sua proteção

Intrusões e Segurança

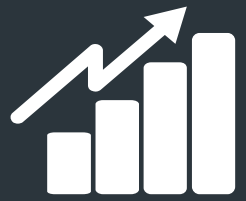
Utilizando uma base sólida para isso, podemos obter informações valiosas sobre o funcionamento e a necessidade de proteção contra intrusões.

As intrusões e anomalias que ocorrem na rede podem ser detectadas durante o tráfego, requerendo o uso de algoritmos para essa finalidade.

INTRUSÕES E SEGURANÇA

DADOS

Todas essas anomalias devem ter uma origem, e é necessário coletar os dados relacionados a elas. Para esse fim, podemos utilizar um protocolo chamado Netflow.



DETECÇÃO

O estudo realizado por Hou et al. (2018) tem como objetivo desenvolver um sistema de detecção de ataques DDoS utilizando técnicas de aprendizado de máquina.

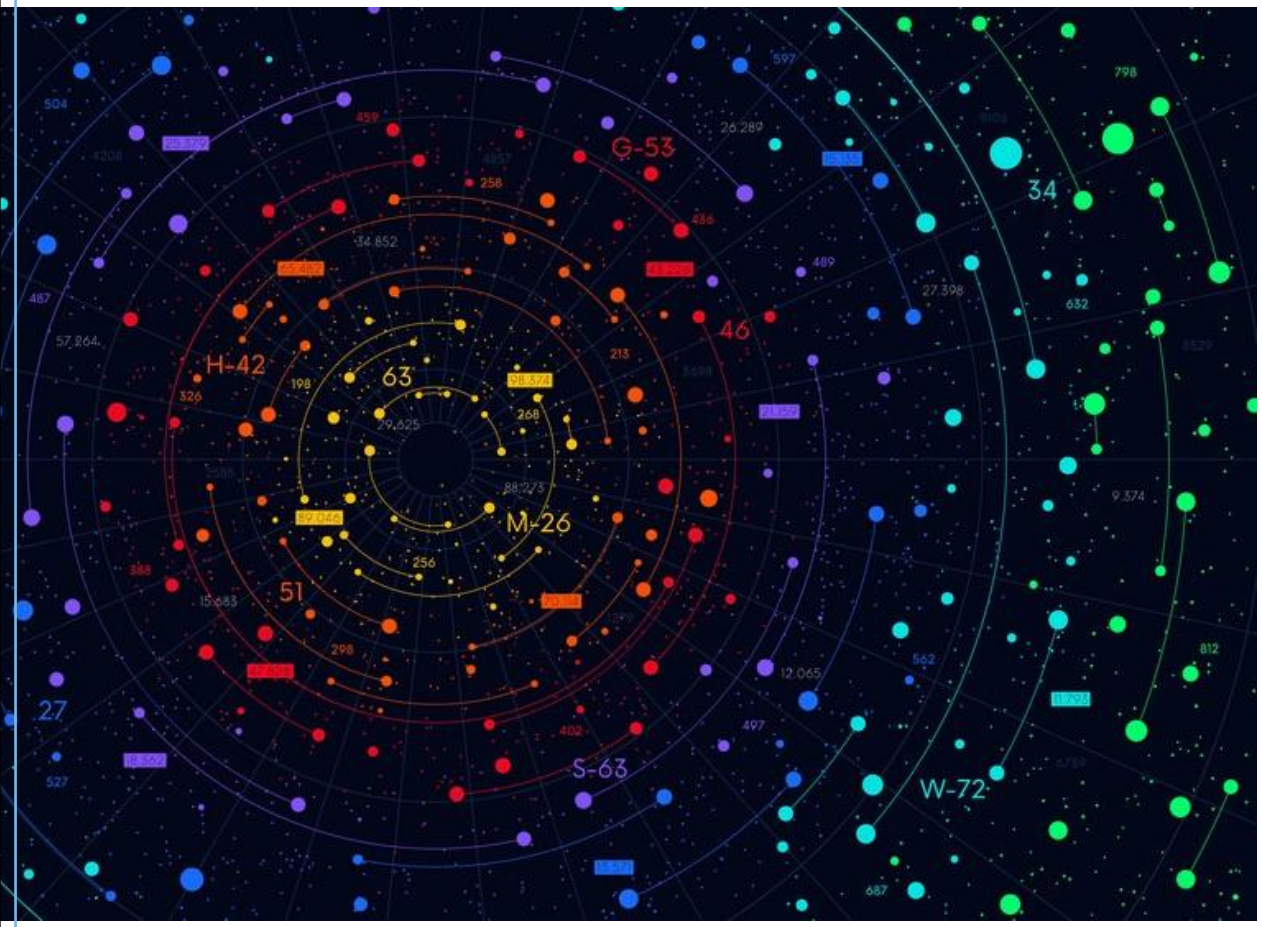
PREDIÇÃO

O estudo de Raja et al. (2022), que explorou o uso de técnicas de aprendizado de máquina para prever ataques cibernéticos.

SELEÇÃO

O estudo de Saber, Abbas e Fergani (2020), que propôs um sistema de detecção de ataques DDoS utilizando algoritmos genéticos híbridos para a seleção ótima de conjunto de características

INTRUSÕES E SEGURANÇA



Conjuntos de Dados

Mencionamos o estudo realizado por Sarhan et al. (2023), no qual foram disponibilizados conjuntos de dados de fluxo de rede (NetFlow) para o treinamento de sistemas de detecção de intrusões baseados em aprendizado de máquina. Exploramos a forma como esses conjuntos de dados podem ser utilizados para aprimorar a eficiência e a precisão dos sistemas de detecção.

APRENDIZADO DE MAQUINA

Em resumo, até o momento, abordamos principalmente o tema do aprendizado de máquina aplicado à detecção de ataques cibernéticos.

Essa abordagem visa identificar comportamentos maliciosos e contribuir para a proteção efetiva de redes e sistemas.

APRENDIZADO DE MAQUINA

Estudo 1

Faz uma abordagem baseada em análise de componentes principais (PCA) para detectar ataques DDoS de camada de aplicação lentos.

Por que?

Artigos científicos são preferíveis por sua credibilidade, rigor metodológico e referências confiáveis. E com isso, os dados vem em conjunto.

E agora?

Com base nesses estudos, a aplicação será embasada neles, facilitando a seleção das bases de dados e algoritmos.

Estudo 2

Fornecimento de conjuntos de dados de fluxo de rede para treinamento de sistemas de detecção de intrusões baseados em aprendizado de máquina.

Redução

PCA é utilizado para reduzir a dimensionalidade dos dados, simplificando a análise e mantendo informações importantes.

ESTUDOS E REFERÊNCIAS

Com base em minhas pesquisas, apresentarei referências de estudos relevantes que contribuem para a cibersegurança e o desenvolvimento de inteligência artificial, a fim de aprimorar a detecção de ataques. Essas referências serão fundamentais para embasar nossa abordagem.

ESTUDOS E REFERÊNCIAS

REFERENCIAS

CORSINI, Andrea; YANG, Shanchieh Jay; APRUZZESE, Giovanni. On the evaluation of sequential machine learning for network intrusion detection.

DAS, Rammanohar; SANDHANE, Raghav. Artificial intelligence in cybersecurity.

FOSIĆ, Igor et al. Anomaly detection in NetFlow network traffic using supervised machine learning algorithms.

HOU, Jiangpan et al. Machine learning-based DDoS detection through.

RAJA, Mr.S.S.Vasantha et al. Prediction of cyber attacks using machine learning technique.

SABER, Abid; ABBAS, Moncef; FERGANI, Belkacem. A DDoS attack detection system: Applying a hybrid genetic algorithm to optimal feature subset selection.

SARHAN, Mohanad et al. NetFlow datasets for machine learning-based network intrusion detection systems.

SILVA, Nícolas Rocha e; SALLES, Ronaldo Moreira. Métricas para a detecção de ataques DDoS.

WATKINS, John; TUMMALA, Murali; MCEACHEN, John. A machine learning approach to network security classification utilizing NetFlow data.

Thanks

THANK YOU FOR LISTENING