Faculdade de Tecnologia de Americana

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

BRUNA MIRELA PEREIRA
MAURO EDUARDO RODRIGUES MAGALHÃES

INTELIGÊNCIA ARTIFICIAL PARA APLICAÇÕES DE SEGURANÇA DA INFORMAÇÃO

Americana, SP
2021

Faculdade de Tecnologia de Americana

BRUNA MIRELA PEREIRA
MAURO EDUARDO RODRIGUES MAGALHÃES

INTELIGÊNCIA ARTIFICIAL PARA APLICAÇÕES DE SEGURANÇA DA INFORMAÇÃO

Projeto monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Professor Marcus Vinícius Lahr Giraldi.

Área temática: Inteligência Artificial.

Americana, SP
2021

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

P489i PEREIRA, Bruna Mirela

Inteligência artificial para aplicações de segurança da informação. / Bruna Mirela Pereira, Mauro Eduardo Rodrigues Magalhães – Americana, 2021.

38f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinicius Lahr Giraldi

1 Segurança em sistemas de informação 2. Inteligência artificial I. MAGALHÃES, Mauro Eduardo Rodrigues II. GIRALDI, Marcus Vinicius lahr III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Bruna Mirela Pereira

Mauro Eduardo Rodrigues Magalhães

INTELIGÊNCIA ARTIFICIAL PARA APLICAÇÕES DE SEGURANÇA DA INFORMAÇÃO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 14 de junho de 2021.

Banca Examinadora:

_____
Marcus Vinícius Lahr Giraldi (Presidente)
Especialista
FATEC Ministro Ralphi Biasi

_____
Jonas Bode (Membro)
Especialista
FATEC Ministro Ralphi Biasi

_____
Mariana Godoy Vazquez (Membro)
Doutora
FATEC Ministro Ralphi Biasi

DEDICATÓRIA

Dedico este trabalho à Sueli e à Luciana, nossas mães, que sempre estiveram ao nosso lado nos incentivando e apoiando na conclusão de nosso trabalho.

AGRADECIMENTO

Primeiramente agradecemos à Deus, aos nossos colegas de sala, e aos professores Marcus Vinícius Lahr Giraldi e Daives Arakem Bergamasco, que compartilharam seus conhecimentos durante a execução de nosso projeto. Conhecimentos estes que foram fundamentais para a finalização e aprimoramento deste trabalho.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

APIS	Interface de programação de aplicações
DNN	Rede Neural Profunda
GPU	Unidade de Processamento de dados
IA	Inteligência Artificial
IBM	International Business Machines Corporation
IOT	Internet das Coisas
ITU	União Internacional de Telecomunicações
PIN	Número de Identificação Pessoal
SI	Segurança da Informação
SIEM	Security Information and Event Management
TI	Tecnologia da Informação

RESUMO

A Inteligência Artificial vem em constante evolução desde 1956. Com seus campos sendo cada vez mais explorados, sempre visando uma inovação e transformação no mundo tecnológico. Com estudos neurológicos e com base na análise humana, essa tecnologia procura sempre evoluir com ações do cotidiano, que ajudam o ser humano nas atividades do dia a dia. Nos dias atuais percebe-se uma presença da I.A. nas atividades realizadas em uma sociedade moderna, tornando processos que antes era necessário ações humanas, se tornando automatizadas por essas máquinas inteligentes. Com toda essa transformação é necessária uma Segurança dessa tecnologia, pois muitas vezes essas máquinas podem se tornar vulneráveis e tomar decisões precipitadas e equivocadas. Apesar desse grande desafio que fabricantes possam enfrentar para implementar a Segurança das aplicações desenvolvidas e atualizadas, a importância da proteção e privacidade dos dados é indiscutível. Os *stakeholders* tem um papel importante a ser trabalhado e discutido em conjunto, para entregar essas aplicações com tecnologias inovadoras a seus clientes, visando a qualidade e a Segurança. Para assim, essas novas tecnologias serem utilizadas em um ambiente íntegro e seguro, visando um menor esforço manual para o ser humano, com atividades sendo executadas com qualidade por essas máquinas inteligentes.

Palavras-Chave: Inteligência Artificial; Segurança da Informação; Privacidade dos Dados.

ABSTRACT

Artificial Intelligence has been in constant evolution since 1956. With its fields being increasingly explored, always senior an innovation and transformation in the technological world. With neurological studies and based on human analysis, this technology always seeks to evolve with everyday actions that serve the human being in daily activities. Nowadays, the presence of the A.I. in the activities carried out in a modern society, making processes that previously required human actions, becoming automated by these intelligent machines. With all this transformation, security of this technology is necessary, as these machines can often become vulnerable and make hasty and wrong decisions. Despite this great challenge that manufacturers face to implement the security of developed and updated applications, the importance of data protection and privacy is indisputable. Stakeholders have an important role to be worked on and discussed together, to deliver these applications with innovative technologies to their customers, qualified for quality and safety. Therefore, these new technologies are used in an entire and safe environment, with less manual effort for the human being, with activities being performed with quality by these intelligent machines.

Keywords*: Artificial Intelligence; Information Security; Data Privacy.*

SUMÁRIO

1 INTRODUÇÃO

A Inteligência Artificial (I.A) pode abranger vários aspectos, como exemplo: lógica, probabilidade, matemática e vai muito além da percepção, raciocínio, aprendizado e ação. Com o passar dos anos surgem pensamentos sobre como entender, compreender algo ou agir. Utilizando a Inteligência Artificial vai muito mais além, ela não procura somente compreender ações humanas, mas sim construir máquinas inteligentes, que possam reproduzir e ajudar nas atividades do dia a dia. (NORVIG e RUSSEL, 2013).

Segundo William Stallings (2014), uma boa segurança visa alcançar os objetivos de preservar a integridade, disponibilidade e a confidencialidade dos recursos de Sistemas da Informação. Esses três componentes são chamados de coração da Segurança de Computadores. A confidencialidade assegura que essas informações estejam seguras e que sejam confidenciais, assegurando que indivíduos não autorizados não tenham acesso a tal informação. Com a integridade temos a integridade de dados (programas são modificados apenas com autorização), e integridade do sistema (assegura que um sistema possa ser executado de forma livre de manipulações). E a disponibilidade, que o serviço sempre esteja ativo e operando normalmente para que seus serviços não fiquem indisponíveis para usuários autorizados.

Conforme Longinus Timochenco (2020), é necessário certa agilidade dos serviços existentes na organização, para que as informações sejam protegidas de possíveis crimes virtuais. Utilizando somente serviços confiáveis para uma proteção da rede, evitando assim possíveis vulnerabilidades, para que a segurança dos dados não seja colocada em risco. Com a utilização de softwares que utilizem a Inteligência Artificial (I.A), é possível combater os criminosos virtuais com mais eficiência, assim tendo uma maior proteção da segurança de informação.

A I.A pode ser utilizada como ferramenta para defender as organizações de possíveis ataques. Os chefes de negócios da segurança da informação analisam o negócio e verificam quais são os possíveis riscos, para assim saber exatamente quais medidas adotar para combater e prevenir possíveis ações de criminosos.

São utilizadas aplicações de I.A para suporte a negócios em várias áreas, como por exemplo: atendimento ao cliente, detecção de fraudes bancárias, entre outras aplicações que ajudam nas atividades humanas.

Segundo Mundo Mais Tech (2020), com a utilização cada vez mais frequente da computação em nuvem, os dados podem ficar comprometidos. Com isso é possível criar aplicações que ajudam na identificação de ameaças com I.A e *Machine Learning*. Com a

utilização de algoritmos que possam ajudar no combate de crimes cibernéticos e, na proteção de dados sigilosos que possam comprometer a integridade de suas informações.

2 INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (I.A) pode ser definida como um estudo de um agente que tem percepções de um ambiente, e executa ações ensinadas de um humano para uma máquina inteligente. Nada mais é do que o aprendizado de uma máquina que procura repetir ações humanas. Há anos a espécie humana procura entender seus pensamentos e percepções. Na I.A vai um passo além: além de entender, ele procura construir máquinas inteligentes.

Existem vários campos dentro da I.A que cobre uma ampla gama de campos. Ela pode ser utilizada em jogos, no ramo da saúde para ajudar a encontrar precipitadamente algumas doenças, no ramo de aplicações que podem ajudar a empresas em gerais a proteger a Tecnologia de seu ambiente corporativo, e pode ser realizada as demais tarefas que possam envolver o "pensar" e "agir" do ser humano.

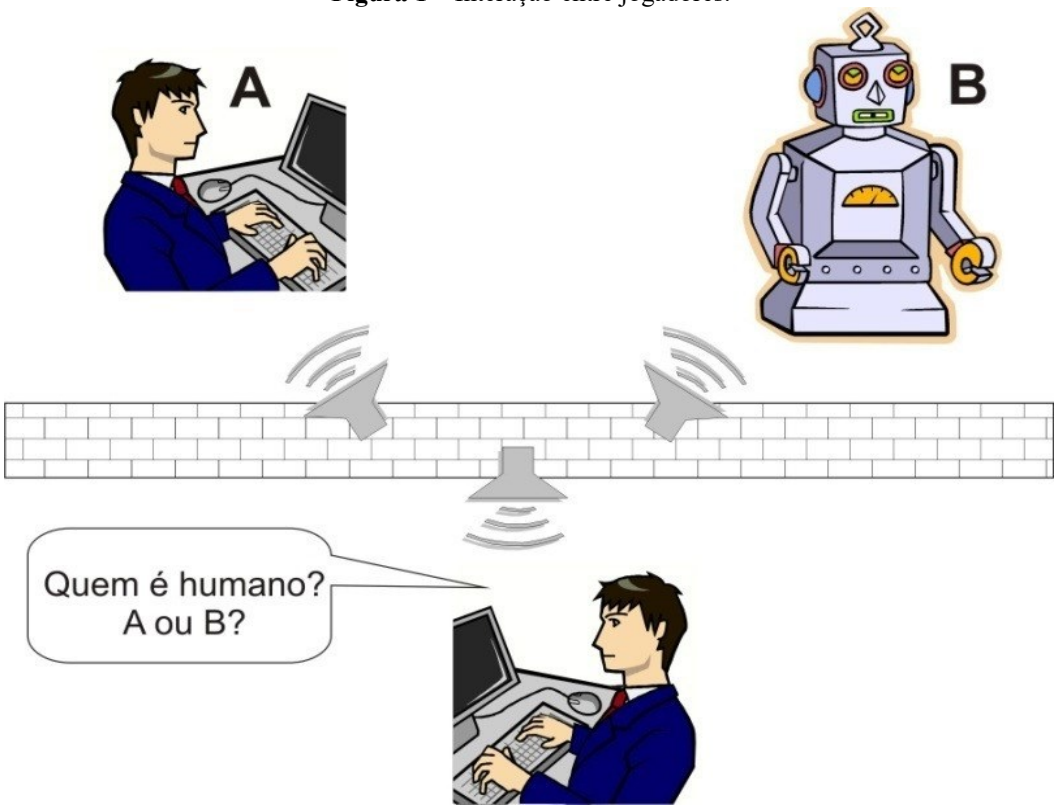
Podemos concluir que tal software possui pensamentos parecidos com um humano. Os pensamentos da mente humana são fundamentais para um estudo mais profundo sobre o assunto. Procurando separar determinados pensamentos, sabendo filtrá-los de maneira que consiga se comparar e uni-los a ações humanas. Vários estudos podem ajudar a entender como realmente funciona a mente humana, para assim poder encontrar formas com que possa tornar equivalente suas ações e pensamentos com algum software de computador por exemplo. É como se algumas ações do software, pudesse manipular comportamentos que pareçam cada vez mais reais. (NORVIG e RUSSEL, 2013).

2.1 Sistemas com ações humanas

O teste de Turing (TURING, 1950) visa formar uma definição eficiente de inteligência. Turing definiu um comportamento como sendo uma capacidade do sistema de obter um desempenho sobre as palavras "máquina" e "pensar", tentando encontrar uma resposta para determinada pergunta, sobre o pensar de uma máquina. Comparando o grau das tarefas cognitivas a tarefas humanas, visando alcançar o objetivo de enganar quem está interrogando a máquina. A ideia do teste se baseia em uma pessoa interrogar um computador, sem saber que está falando com a máquina, conforme exemplo na Figura 1. Quem interrogar o computador, pode escolher as perguntas em questão, visando tentar diferenciar se pode estar conversando com uma pessoa ou uma máquina. Seria aprovado o teste no computador se a pessoa em questão

não alcançasse o objetivo de identificar que estava ou não falando com um computador ou um humano, que não soubesse diferenciar.

Figura 1 – Interação entre jogadores.



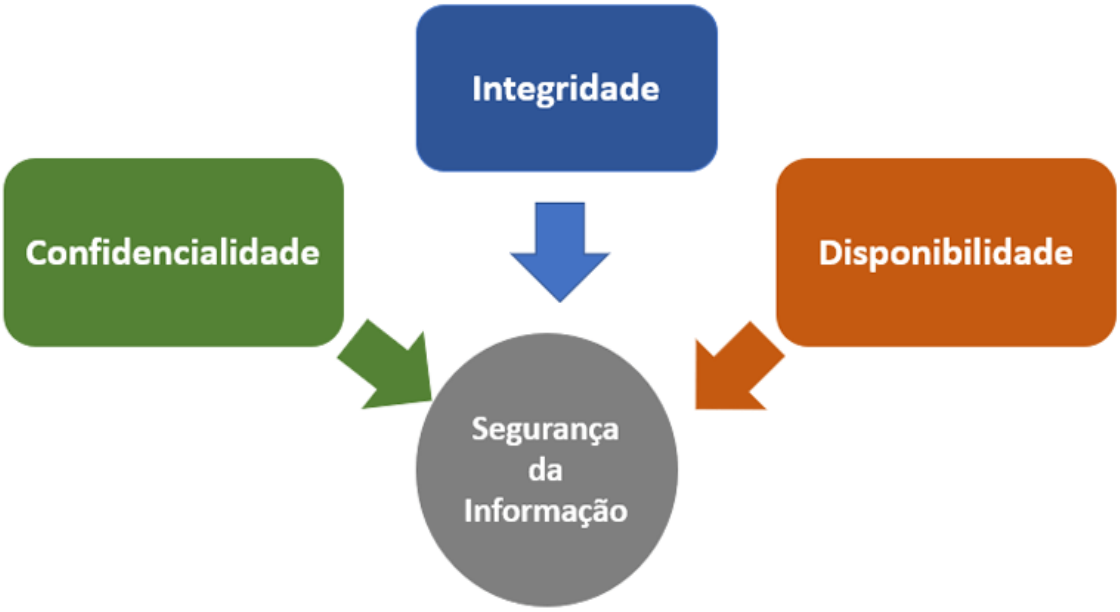
Fonte: MACHADO, 2020, p. 8.

2.2 O que é Segurança da informação?

A Segurança da Informação (S.I) procura preservar a integridade, disponibilidade e a confidencialidade de Sistemas da Informação, como: hardware, software, informações e dados, como o exemplo da Figura 2. Procura-se utilizar métodos para proteger sua informação de possíveis hackers e criminosos, que de alguma forma tentam roubar informações sigilosas. Com esses métodos é possível minimizar os riscos existentes, e proporcionar uma maior segurança no ambiente. Uma organização visa sempre proteger seus ativos, pois uma informação vazada sem os cuidados necessários pode causar grandes prejuízos a organização. Hackers utilizam vários métodos para tentar obter informações, de forma que o usuário não desconfie. Com isso, é interessante a empresa tentar proteger seus ativos da informação através de treinamentos para seus funcionários, implementar políticas de segurança, e tentar sempre manter suas informações em sigilo, para que um vazamento indevido não ocorra. O maior desafio da área de S.I vai muito além de software ou hardware. A maior vulnerabilidade encontrada nesse aspecto, é a

vulnerabilidade humana. Com isso, a organização tem que encontrar formas para que seu funcionário mantenha em sigilo informações confidenciais da empresa e de seus bens. Procurando sempre os informar e fazê-los entenderem tamanha responsabilidade de cada informação. Qualquer ato irresponsável poderá fazer a empresa perder sua reputação. Mas, com a dedicação e desempenho de toda equipe, e sabendo como agir a determinadas situações, a empresa tem tudo para conseguir o entendimento de todos que fazem parte da organização ou até mesmo fora dela, sobre o quão importante é a Segurança da Informação (STALLINGS, 2014).

Figura 2 - Princípios básicos Segurança da Informação.



Fonte: https://www.techtem.com.br/principios-basicos-da-seguranca-da-informacao/

2.3 Inteligência Artificial em Segurança Cibernética

Os Sistemas que utilizam a Inteligência Artificial ainda possuem algumas falhas, porém com a utilização da I.A é possível prevenir muitos crimes cibernéticos. Alguns componentes que podem fazer com que a I.A possa falhar é o campo da automação, onde podem ocorrer testes falsos positivos. Computadores são programados para executarem automaticamente tarefas diárias, que inclui analisar o tráfego da rede, com base em regras para detecção de anormalidades no sistema. Profissionais de Segurança Cibernética trabalham para o desenvolvimento de algoritmos, e investigação de novas ameaças que possam comprometer a integridade dos sistemas. Fazem com que esses algoritmos possam remover falsos positivos, sendo essencial para que a I.A possa assumir o futuro. Alguns campos podem ser analisados de

uma melhor forma, pois ataques se tornam cada vez mais comuns atualmente, e avançam em termos relacionamentos a complexidade. A I.A vem para ajudar, com seu monitoramento inteligente, analisando e identificando padrões de alguma atividade suspeita ou maliciosa.

Com o uso adequado da I.A pode-se identificar atividades em estágios iniciais de um ataque, ajudando a localizar o ataque e neutralizá-lo. A I.A é treinada como um sistema imunológico do corpo humano, e por isso é capaz de neutralizar as ameaças de uma forma eficaz. Os glóbulos brancos e os anticorpos conseguem neutralizar as ameaças que não são conhecidas, sem desligar o sistema por completo. O sistema pode aprender com experiências e ficar mais forte, assim como o organismo fica após uma infecção. Em sistemas de Segurança possivelmente lentos e insuficientes, pode-se aplicar a I.A para melhorar o desempenho da Segurança e toda proteção a ameaças cibernéticas. Com uma investigação mais profunda, o sistema imunológico comparado aos sistemas de I.A possuem duas estruturas utilizadas: as redes neurais e sistemas especialistas. As Redes Neurais são modelos que imitam uma estrutura e a função do cérebro humano, e os sistemas especialistas são sistemas de Software que podem localizar respostas, e consultar algum domínio de algum aplicativo permitido por um usuário ou por outro sistema de Software.

O mais recente *"Deep Neural Network"* (Rede Neural Profunda, DNN) é utilizado não apenas para proteger as organizações, mas para prever esses ataques. A I.A utilizada em ferramentas ou sistemas, podem consistir em dois tipos: fundamentados em casos de raciocínio e sistemas baseados em regras. Os raciocínios são baseados em casos que permitem a resolução de problemas, que podem relembrar problemas semelhantes aos casos. Casos que já foram solucionados e executados pela máquina antes, são utilizados como modelos que podem solucionar problemas. Os sistemas que são baseados em regras, podem resolver os problemas com essas regras definidas pelo especialista. Regras definidas pelos especialistas podem ser definidas em duas partes: A condição e a ação. Sendo a condição avaliada, para assim poder definir que tipo de ação deve ser tomada (CHAN; SIMON; MIN *et al,* 2019).

A I.A. é utilizada em muitos negócios para organizações. Chefes de organizações procuram verificar quais são os riscos da organização, e com isso utilizam a I.A. para ajudar a combater possíveis vulnerabilidades encontradas. Existem muitas aplicações nos dias de hoje que utilizam a Inteligência Artificial. Várias empresas utilizam dessa tecnologia para garantir sistemas inteligentes que possam facilitar o funcionamento de seus serviços. Um exemplo bem utilizado é o reconhecimento facial, utilizado não só em empresas, mas sim em aplicações que garantem uma maior eficiência e segurança aos seus softwares. Câmeras de Segurança também são bastante utilizadas para proteção de vários ambientes. Nos dias atuais cada vez há avanços

na tecnologia, que fazem com que grande parte da população faça um investimento nessas aplicações (PINTO, 2019).

A utilização da Inteligência Artificial, tem por finalidade proteger o negócio e manter seguro as aplicações do ambiente. Uma forma utilizada inclui aplicações que envolvem o atendimento ao cliente. Como exemplo: ligações que caem em correios de voz, sendo possível que o cliente digite uma opção e seja direcionado até determinado setor responsável. Com isso é possível diminuir o tempo de espera do mesmo, e os atendentes ficam livres para outras ligações, sendo assim indispensável a utilização dos sistemas para que seu negócio melhore e tenha uma rápida resolução do problema de seu cliente (TIMOCHENCO, 2020).

A IBM é uma das maiores empresas de Tecnologia do mundo, onde possui muitas aplicações no mercado. Segundo sua política de privacidade dos dados, a empresa prioriza seu cliente fornecendo serviços altamente seguros que façam com que eles se sintam seguros em guardar seus dados sigilosos, fazendo assim com que tenham confiança nos serviços que a empresa fornece. Como parte de seus negócios, a IBM prioriza a criptografia, não repassando ou fornecendo qualquer chave que leve uma pessoa não autorizada a ter acesso a qualquer informação que seja fornecida por seus clientes. A segurança é essencial e priorizada, parcerias que ajudem a alertá-los sobre possíveis ações não autorizadas são aceitas, ajudando na prevenção de possíveis ataques.

A empresa entende que nenhuma máquina poderá substituir ações humanas ou decisões que as pessoas podem tomar, mas acreditam que poderão alcançar grandes resultados com seus códigos bem elaborados, para assim ajudar na tomada de decisões. A automação faz parte do planejamento da IBM, pois ela acredita em sua grande capacidade de ajuda e eficiência nos negócios (IBM, 2017).

Segundo a empresa Stefanini (2020), os *chatbots* são programados para que se assemelhem a conversas naturais, são programados para isso. É um exemplo bem utilizado pelas empresas atualmente, para facilitar o trabalho e experiência do usuário. O grande desafio é fazer uma interface bem intuitiva para chamar a atenção do mesmo, até mesmo com *chatbots* que podem ser utilizados em conversação, para melhorar a comunicação e compreensão de seu usuário.

Aplicações de gestão também são bem utilizadas por organizações, podem ser utilizadas para medir o progresso e eficiência de cada funcionário da empresa, para verificar se suas tarefas estão sendo bem executadas. A equipe da gestão pode utilizar o meio da Inteligência Artificial com o método de auxiliar nas decisões, com informações que podem ajudar a tomar decisões precisas.

A assistente pessoal é bem utilizada, não somente por organizações, mas em todos os tipos de dispositivos. Uma assistente pessoal bem conhecida é a Siri, utilizada por dispositivos da Apple. É um software que pode identificar um comportamento pessoal, e ajudar o usuário da aplicação com informações, por conta de seu aprendizado de máquina. Bancos também utilizam aplicações para ajudar o usuário a realizar tarefas com mais eficiência e rapidez.

Na parte de segurança pode-se utilizar a I.A a favor de quem procura uma proteção a sua rede. Os ataques são cada vez mais frequentes quando se fala do mundo digital. Um ataque bem conhecido é o ataque em aplicações que utilizam o Internet Banking. Utilizando a I.A como meio de proteção, pode-se realizar combinações que ajudam na identificação de um ataque a vários servidores, e com isso uma maior agilidade na resposta. Sistemas que utilizam a I.A são rápidos e eficazes, e com isso dificulta a vida do Hacker.

2.4 Sistema de treinamento de máquina

Um exemplo de sistema bem conhecido e utilizado no treinamento de máquina, é o Watson da IBM (*International Business Machines Corporation*). Ele é uma Inteligência Artificial que pode ser utilizado em ambientes de nuvem. São ensinados conhecimentos para o mesmo, com isso sua ajuda no desenvolvimento de aplicações pode transformar os processos automatizados, fazendo com que usuários em geral tenham essa interação com a aplicação.

Pode-se utilizar o Watson como um assistente de *ChatBot*, que o usuário encontra dúvidas sobre aplicações utilizadas em sua empresa. Dentro dessa aplicação são ensinados e configurados vários algoritmos, que ajudam na facilitação e no compreendimento das perguntas de seus usuários. Com essa interação, empresas podem ganhar com o rápido entendimento dos problemas relacionados a determinados departamentos, e com isso ganhará agilidade no processo (IBM, 2020).

3 APRENDIZADO DE MÁQUINA (MACHINE LEARNING)

Com o aprendizado de máquina *(Machine Learning)*, pode-se utilizar algoritmos que fazem com que a máquina “aprenda” determinadas ações. Com esses algoritmos é possível que ela saiba responder a questões diferentes e tomar diferentes decisões e escolhas.

Seu sistema de aprendizado não é igual a uma programação comum, neste método são criadas algumas condições, fazendo com que o usuário interaja com o programa, gerando uma saída. No aprendizado de máquina, somente no fim da introdução de seus dados são gerados suas condições e seu algoritmo. Realizando toda uma separação de seus componentes, estudando todas as informações apresentadas e somente por último, seu algoritmo é criado com suas próprias regras (IBM, 2020).

Conforme Turing (1950), existem entidades que separam a mente humana da máquina, e o intuito é encontrar soluções para tornar semelhante o entendimento de ambas. Encontrar condutas de uma mente ao pensar, conseguir encontrar uma resposta para pergunta em questão. Algo que a faça ter dúvidas e encontrar algumas críticas e opiniões dentro de sua mente. Várias ideias percorrem e questionam a mente humana, pensando em como obter uma resposta. Se é possível pensar, é possível com os mesmos ensinamentos fazer uma máquina pensar. Ao pensar é possível obter informações distintas, portanto toda mente tem um pouco da mecânica, cabe apenas fazer com que a máquina consiga assimilar-se cada vez mais a uma mente humana.

Segundo Hurwitz e Kirsch (2018), *Machine Learning* vem se tornando cada vez mais importante para os negócios, sendo uma maneira de proteger os ativos da organização. Com a medida correta e alterações de determinadas tecnologias, a empresa tem tudo para deixar informações e dados altamente seguros. Ambos pensam como algo que pode ser utilizado e sempre atualizado, com o estudo e conhecimento apropriado pode ajudar sobre possíveis ações futuras. Diferencia-se da programação comum, tendo em vista que pequenos dados são ensinados a máquina, com combinações que fazem com que o sistema fique cada vez mais inteligente e possa dar informações mais precisas a seus usuários. Quanto mais informações forem ensinadas a máquina, mais precisa também serão sua tomada de decisão.

3.1 Machine Learning para negócios

Utilizando a Inteligência Artificial, é possível identificar ameaças que ao olho humano é difícil de se detectar. Informações que não podem ser acessadas, muitas vezes são acessadas por criminosos. Com os algoritmos corretos implementados com a *Machine Learning*, é possível evitar perdas de dados sigilosos. A perda de dados pode ser evitada com a tomada de

decisão correta pela máquina, com algoritmos bem estruturados é possível evitar grandes perdas de informações.

Os algoritmos funcionam na base de respostas de uma análise realizada através de sistemas, que identificam algumas regras de perguntas e interações do ser humano.

Para empresas, utilizar *Machine Learning* é fundamental para os negócios. Com ela é possível executar algoritmos seguros, para que com isso possa facilitar os negócios da empresa (IBM, 2020).

3.2 Machine Learning para área da saúde

Pode-se utilizar a I.A para resolver problemas para tratamento de pacientes, na área da saúde. Com questões sobre como realizar o tratamento dos pacientes, e seu maior desafio é conseguir identificar o melhor tratamento que tenha mais eficiência para cada paciente, pois nem todos possuem as mesmas características, e com isso alguns medicamentos podem dar efeitos colaterais em determinados pacientes, e em outros não, porém os tratamentos são altamente eficazes. Dentre os medicamentos, pode-se observar a faixa etária, o sexo da pessoa, para assim verificar os efeitos colaterais dos medicamentos. Com alguns métodos de regressão e classificação de algoritmos, pode construir tratamentos bem eficazes que cause bons resultados em seus pacientes. Para se utilizar um modelo de regressão, se identifica mudanças no estado do paciente ao ingerir determinado medicamento. Com a criação desse algoritmo no aprendizado de máquina, pesquisadores podem conseguir identificar como os pacientes reagem a determinados medicamentos. E com isso, observa-se a identificação desse medicamento e como ele age no corpo humano. A máquina ajuda a identificar o perfil de cada paciente, e com isso indicar o medicamente que agiria melhor em seu corpo.

Vários aplicativos cognitivos, mais conhecidos como APIs (Interface de programação de aplicações), podem conter interfaces intuitivas que facilitam o médico em questão a se comunicar com a máquina. Realizando várias perguntas para assim poder garantir um melhor tratamento para o perfil de cada paciente, garantindo o menor efeito colateral possível (HURWITZ E KIRSCH, 2018).

3.3 Inteligência Artificial para Internet das coisas (IoT)

Os sensores são ligados à Internet das coisas (IoT). Eles são mais baratos atualmente, mas devem ser eficientes para suportar vários dispositivos de uma só vez. Os dados que são produzidos por esses sensores, possuem uma estrutura certa para realizar a aplicação no aprendizado de máquina. Com a grande quantidade de dados produzidos, podem não ser totalmente compreendidos, mas a utilização desses dados com o sensor, em conjunto com os algoritmos de aprendizado de máquina, é possível construir modelos que podem ajudar a prever problemas mecânicos futuros, como a identificação da falha de um processo.

O principal objetivo das organizações é evitar que o sistema fique indisponível. Com a devida atualização de seus sistemas com tecnologias mais recentes, pode-se evitar potenciais falhas nos mesmos. Realizar manutenções preventivas são uma opção, com ela é possível identificar problemas que possam ocorrer no futuro. A IoT pode ser utilizada para agregar dados aos sensores, trazendo uma evolução e facilidade para organização com suas tecnologias atuais. (HURWITZ E KIRSCH, 2018).

3.4 Prevenção de Acidentes

Organizações em geral procuram realizar seus serviços de maneira que, a segurança de suas aplicações esteja trabalhando de forma segura. Os departamentos responsáveis precisam verificar possíveis falhas e vulnerabilidades, e realizar as devidas prevenções em seus sistemas. Mas, muitas vezes e com as devidas precauções, não é o suficiente para um possível incidente.

Às vezes o ambiente fica vulnerável a condições climáticas que podem interferir no funcionamento dos equipamentos. Pode-se fazer o uso de alguns algoritmos que possa identificar condições climáticas, assim ajudando a prevenir possíveis incidentes.

Os algoritmos implementados, serão essenciais para ajudar na detecção de alguma anormalidade no tempo. Seria uma medida importante na prevenção, ao qual evitaria a perda de equipamentos (HURWITZ E KIRSCH, 2018).

3.5 Respostas a incidentes de T.I

Realizar operações de Tecnologia da Informação (T.I) pode ser um pouco difícil, pois envolvem vários dispositivos de rede diferentes, como por exemplo: servidores, computadores, sistemas de armazenamento etc. Os sistemas possuem diferentes meios de gerenciar seus dispositivos, por isso existem várias atualizações de softwares, para assim manter seus dispositivos em perfeito funcionamento. Se caso ocorrer alguma atualização que contém algum

erro, pode afetar uma massa muito grande de clientes, fazendo com que o sistema fique indisponível.

As organizações procuram manter dispositivos para monitorar o funcionamento de suas aplicações. Esses monitoramentos são realizados para buscar capturar e guardar o maior número de dados possíveis, para conseguir identificar os dados do sistema, se possuem alguma anormalidade ou não. Um grande desafio é monitorar todos os acessos, que são exclusivamente monitorados por logs do sistema. Para entender completamente o sistema, os logs devem ser compreendidos. Com um bom monitoramento desses logs das aplicações, é possível encontrar erros e informações que podem ajudar o responsável a corrigi-los e melhorar o desempenho de suas aplicações.

Aplicações que utilizam a I.A permitem que as organizações consigam corresponder com a entrega de um serviço de qualidade, pois com o devido monitoramento, possíveis problemas podem ser corrigidos. Assim, deixando o usuário satisfeito com o serviço disponibilizado.

Outro fato que cientistas de dados estão realizando, é juntar vários algoritmos que possam verificar anormalidades em eventos. Opções podem ser incluídas no aprendizado, como exemplos: alertas, logs, instrumentação ou sensores, ambos criados no data center. O algoritmo cria um modelo, que identifica algumas dependências que estão no elemento que pertencem ao ambiente em si. Também é bem utilizado métodos comparativos, assim que mais informações vão sendo inseridas, conforme vão surgindo novas necessidades de aumento de dados (HURWITZ E KIRSCH, 2018).

3.6 Proteção contra Fraude

Pode-se pensar em detectar uma fraude como um jogo, mas as pessoas que o jogam estão ficando cada vez mais aptas ao jogo de enganar para obter informações. Conforme o tempo vai passando, o aumento de casos no mundo digital cresce, pois as pessoas utilizam cada vez mais o mundo online. Muitas empresas utilizam a Inteligência Artificial, como um meio de bloquear o acesso de intrusos a softwares não autorizados para o uso de terceiros. Uma máquina bem configurada com algoritmos altamente capacitados, permite que a mesma consiga identificar alguma anomalia, e bloqueia imediatamente o acesso desse intruso antes que os estragos possam ser comprometedores.

Proteger informações das organizações se tornou algo cada vez mais difícil, pois é uma longa batalha com variedades técnicas, que ajudam no combate. Alguns algoritmos chamados lineares, foram utilizados durante um certo tempo para separar o grau de atividades. Alguns algoritmos considerados “fracos” podem não conseguir realizar a identificação a tempo, antes que ocorra o desastre. O criminoso pode conseguir alterar sua técnica, e o algoritmo em questão não consegue identificar suas ações, e com isso as informações ficam comprometidas.

O importante é sempre estar à frente do criminoso, assim podendo antecipar suas ações, e sabendo agir em determinadas situações. Fazendo com que o mesmo, não obtenha sucesso utilizando seu método. Por isso, são utilizados algoritmos avançados que permitem a detecção de técnicas altamente fraudulentas. Um exemplo utilizado são as redes neurais, que utilizam aprendizagens bem profundas, que consomem mais dados do que a forma comum de um aprendizado.

Uma organização utilizará todas as formas possíveis de aprendizados em conjunto, para ter uma maior proteção de dados, ou seja, não irá utilizar a rede neural de uma forma que não trabalhe junto com outros algoritmos. O algoritmo linear pode perder um pouco sobre informações referente a informações de uma atividade imprópria. Ele é altamente capacitado para outras funções, mas para descobertas de ações, ele sozinho é insuficiente. O ideal é o modelo final do algoritmo, deve-se incluir todas as formas utilizadas para o aprendizado de máquina, para se tornar assim mais eficiente.

Um exemplo que pode ser utilizado é: um paciente pode obter informação de médicos diferentes. Com isso é possível ligar várias opiniões de pessoas diferentes, e transformar em uma só, tornando a opinião precisa e mais eficiente (HURWITZ E KIRSCH, 2018).

3.7 Previsões do futuro para o Aprendizado de Máquina

A indústria dos testes vem crescendo conforme os anos vão se passando, e a Inteligência Artificial vem como líder no mundo do software. O que no passado se esperava uma certa demora, hoje as coisas são bem diferentes. *Machine Learning* é por sua vez basicamente implementada em aplicativos.

Conforme Hurwitz e Kirsch (2018), com o passar dos anos será possível verificar em várias aplicações a utilização do aprendizado de máquina, tendo a intenção de antecipar o futuro e realizar a criação de uma inovação bem competitiva no mercado. Dispositivos móveis, IoT, e

hubs, terão a implementação dessa novidade. Um exemplo bem conhecido que já mantem a I.A como aplicada em seus negócios, são sites de varejo e anúncios online. Esses modelos são utilizados para proporcionar uma experiência ainda mais agradável para os usuários que utilizam as aplicações.

Um dos principais objetivos, é alterar o modo como o ser humano realiza as atividades atualmente. É bem importante para área da saúde, e pode-se utilizar para medir-se o surto de uma doença transmissível, ou eventos grandes ocorrendo na cidade. Sempre visando resolver e solucionar problemas que as vezes passam a ser imperceptíveis ao olho humano. O valor da organização pode ser amplificado, com base nos serviços e confianças do cliente. Oferecendo serviços com uma maior segurança, e inserindo sistemas inteligentes (HURWITZ E KIRSCH, 2018).

4 APLICAÇÕES DA I.A

À medida que os sistemas de I.A se tornam mais desenvolvidos e novos aplicativos são legalizados, também são desenvolvidas formas mais avançadas de cometer diferentes crimes cibernéticos. Grande parte das corporações já implementou softwares para proteger dados e informações que definem as empresas, mas, para muitas, a carga tributária de instalação dessa proteção é muito alta. Considerando tudo isso, é o dever da corporação aliviar o risco da maneira que puder, portanto, eles devem determinar se esse investimento financeiro é um investimento que vale ou não a pena.

Devido à dependência de conexão com a Internet das Coisas, o custo só aumentará se as empresas não atualizarem com continuidade os sistemas de segurança em paralelo com a evolução das ameaças cibernéticas. Ao aplicar a tecnologia de I.A para proteger os bancos de dados, os programas continuarão a aprender com cada tentativa de ataque, permitindo que evitem qualquer tipo de violação com bastante antecedência. A pesquisa sobre o que as violações estão custando às empresas em todo o mundo, trouxe a ideia de que a I.A está se tornando uma necessidade. As empresas devem considerar o benefício de longo prazo de programas incluindo essa tecnologia.

No entanto, implementar a I.A não é uma maneira muito segura de proteger os bancos de dados do usuário. A tecnologia de I.A tem uma série de preocupações em torno dela, como a falta de código adequadamente adaptado a máquina. Quando se trata de tomar decisões de extrema importância que podem ter impactos específicos, os programas de I.A podem não ser capazes de reconhecer esses impactos potenciais e definir qual seria a decisão mais correta. Os programas não são incapazes de sentir e tomar decisões moralmente corretas. No estágio atual, eles são alimentados apenas pelos dados experienciais e comportamentais usados pelo empregador. Também há uma falta de regulamentação quando se trata de implementar programas de I.A com a segurança cibernética. Devido à liberdade do programa, muitos especialistas temem que tenha algum risco de os humanos perderem a capacidade no processo de tomada de decisão. Essa ideia anda de mãos dadas com a falta de um código moral nos programas. Na maioria das vezes, os programas irão tomar decisões mais comuns e baseadas em dados devido à sua incapacidade de levar as emoções em consideração. Como resultado, as máquinas ainda não são capazes de manter a segurança cibernética de forma autônoma, o que significa que não podem substituir totalmente o modelo de tomada de decisão humana, quando se trata do reconhecimento emocional adequado e da decisão ética adequada, mas no cenário atual de rápido crescimento de *malwares* e ataques cibernéticos mais eficazes, é inevitável a

necessidade de desenvolver formas mais inteligentes de segurança cibernética (CHAN; SIMON; MIN *et al,* 2019).

4.1 IBM SIEM QRadar Advisor with Watson

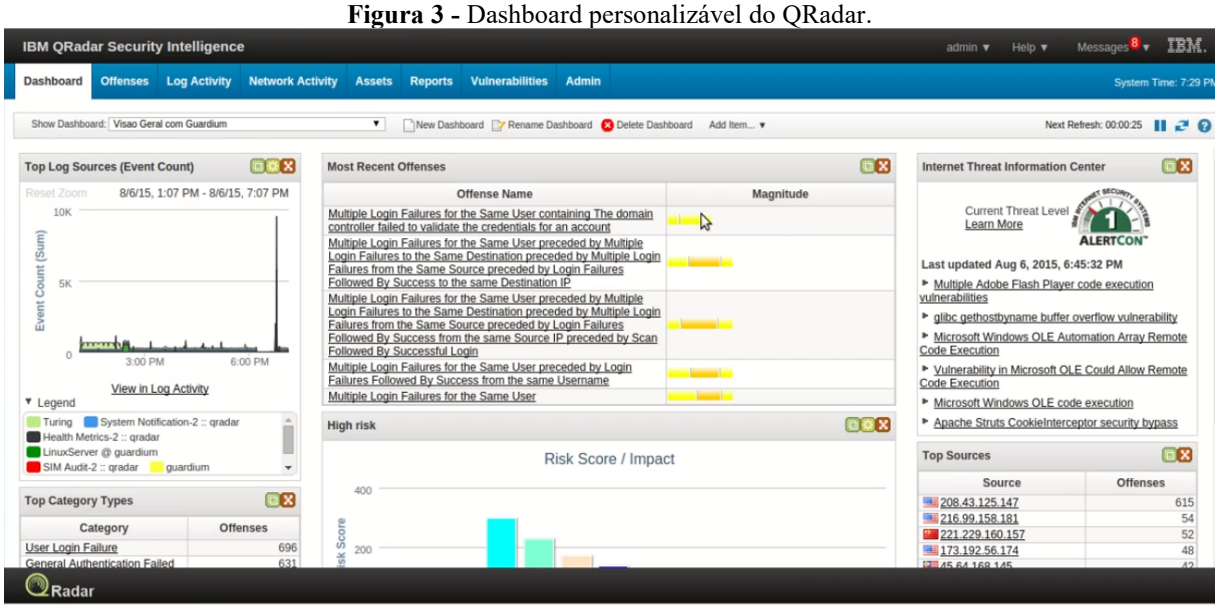
O SIEM (*Security Information and Event Management*) QRadar é uma ferramenta desenvolvida para auxiliar as equipes de segurança a identificar e priorizar com maior precisão as ameaças recebidas diariamente nas empresas. Utilizando insights inteligentes, permite que as equipes consigam responder com mais rapidez aos incidentes, reduzindo o risco e impacto dos mesmos.

A ferramenta consolida logs e dados de fluxo de rede de milhares de dispositivos ao mesmo tempo, ao longo de toda a extensão da rede. O QRadar consegue correlacionar informações diferentes do habitual, e assim criar alertas únicos para facilitar o tratamento e a velocidade de correção do problema identificado.

O Watson da IBM trabalha integrado ao QRadar como mostra a Figura 3. Sua inteligência cognitiva armazena as informações sobre as ameaças e os tratamentos efetuados ao longo do tempo. Sendo assim, possível realizar uma comparação de futuras ameaças com ameaças passadas, trazendo as informações de tratamento utilizadas anteriormente pela equipe de segurança para as ameaças que podem ser similares, facilitando a identificação de problemas parecidos e permitindo que o tratamento seja feito mais rápido, diminuindo o risco e o impacto das ameaças encontradas.

O Watson também pode ser utilizado para automatizar problemas que acontecem diariamente, possibilitando que os operadores possam se concentrar em problemas mais importantes ao longo do dia (IBM, 2021).

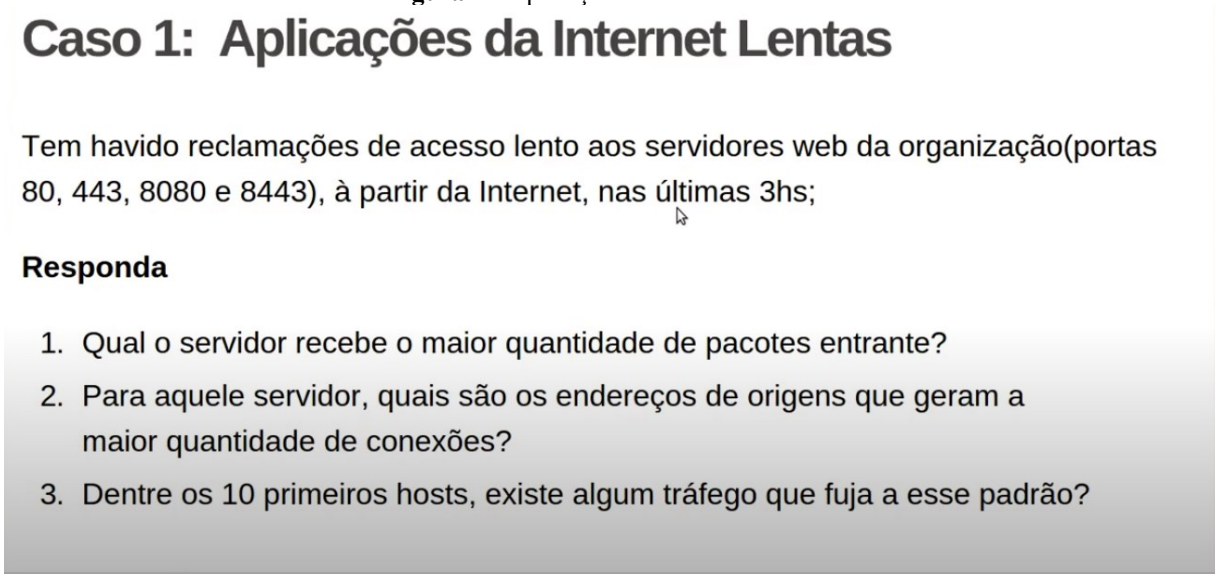
Figura 3 - Dashboard personalizável do QRadar.



Fonte: Vídeo Youtube: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s

Como pode ser observado na Figura 4, existem reclamações de um servidor WEB que está sofrendo lentidão nas últimas 3 horas, sendo tratado pela ferramenta SIEM QRadar:

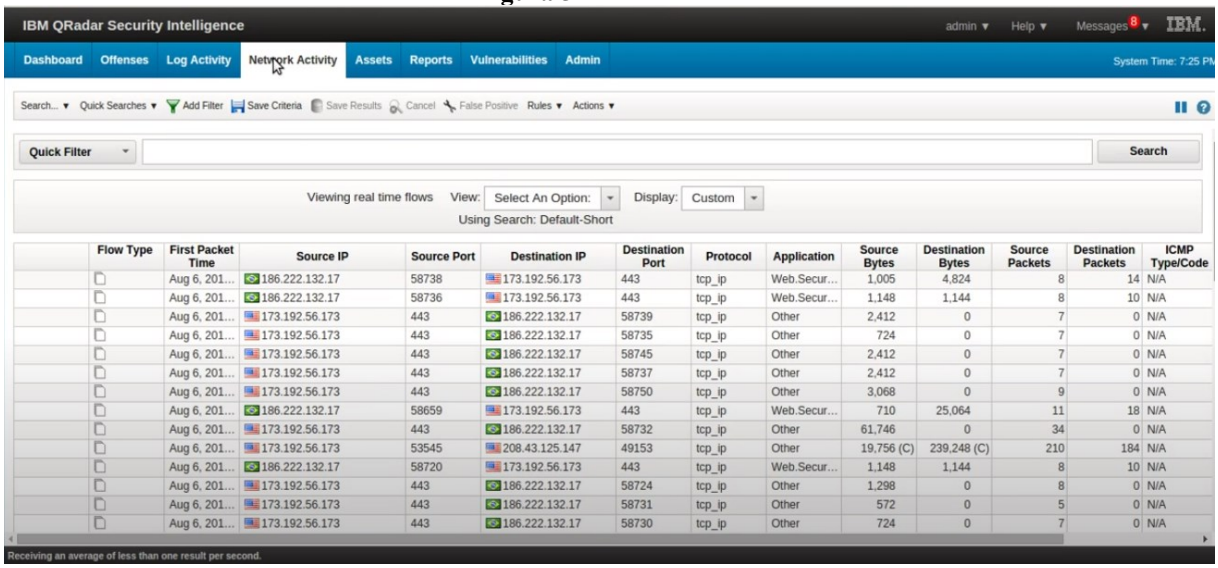
Figura 4 - Aplicações da Internet Lentas.



Fonte: Vídeo Youtube: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s

Na Figura 5 pode ser observada a aba que mostra o fluxo de rede da rede atual utilizada no exemplo.

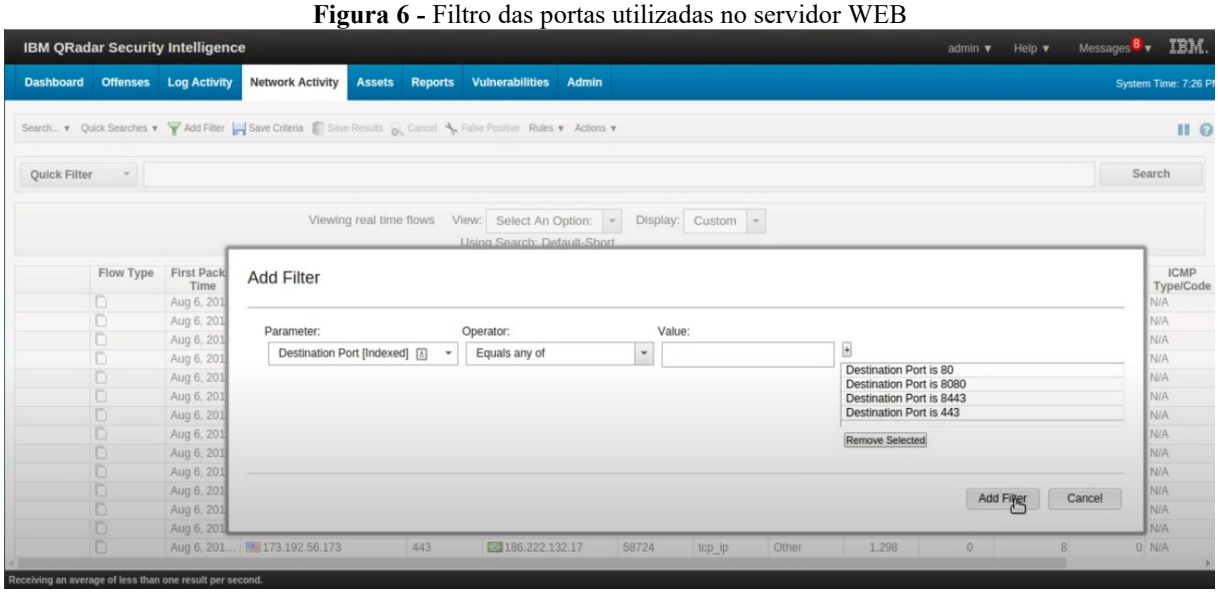
Figura 5 - Fluxo de rede



Fonte: Vídeo Youtube: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s

A Figura 6 mostra a aplicação do filtro apenas com as portas utilizadas no servidor WEB, para a análise específica do que poderia estar acontecendo.

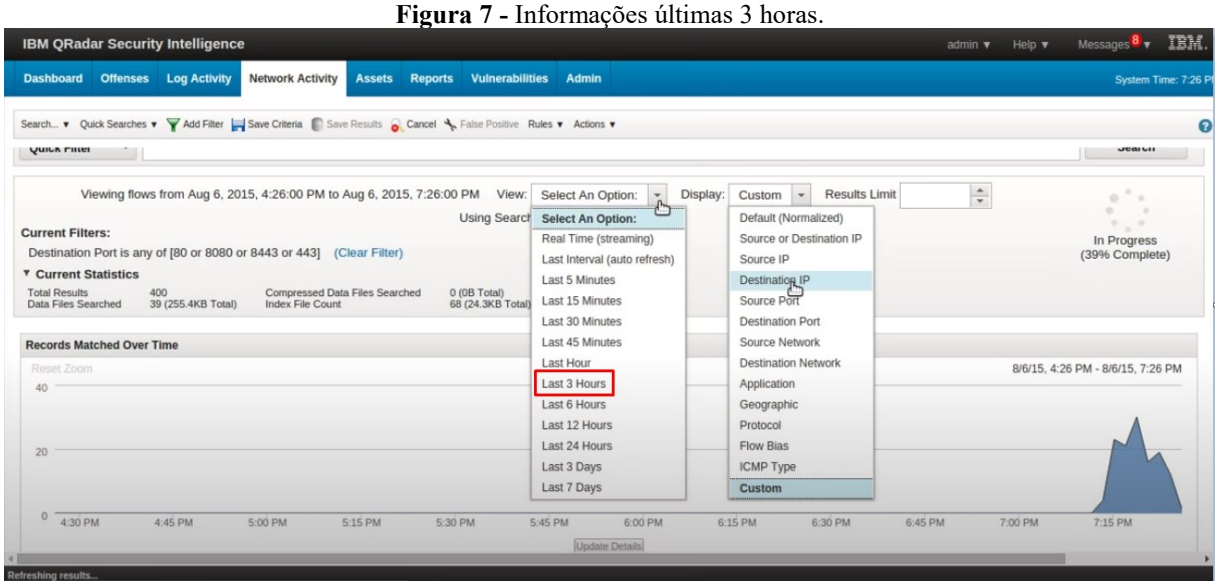
Figura 6 - Filtro das portas utilizadas no servidor WEB



Fonte: Vídeo Youtube: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s

A figura 7 mostra a aplicação de outros filtros para que seja retornado apenas as informações das últimas 3 horas, e por *destination* IP.

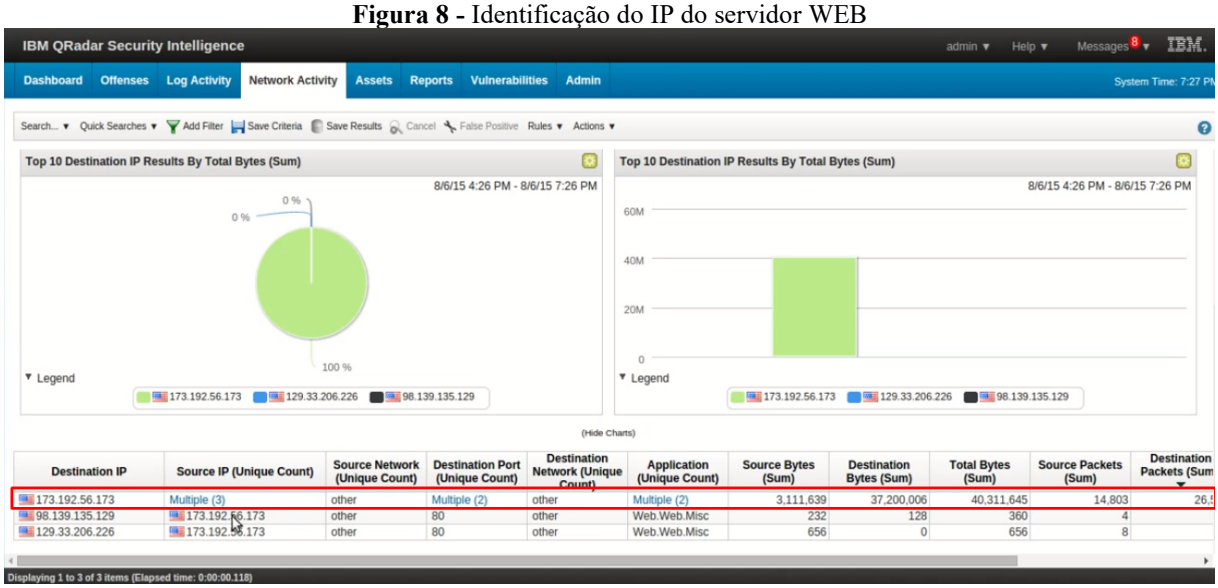
Figura 7 - Informações últimas 3 horas.



Fonte: Vídeo Youtube: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s

O exemplo da Figura 8 mostra a aplicação desses filtros. No exemplo já é possível identificar qual é o IP do servidor WEB que está sofrendo a maior carga de solicitações de acesso, se tornando o gargalo.

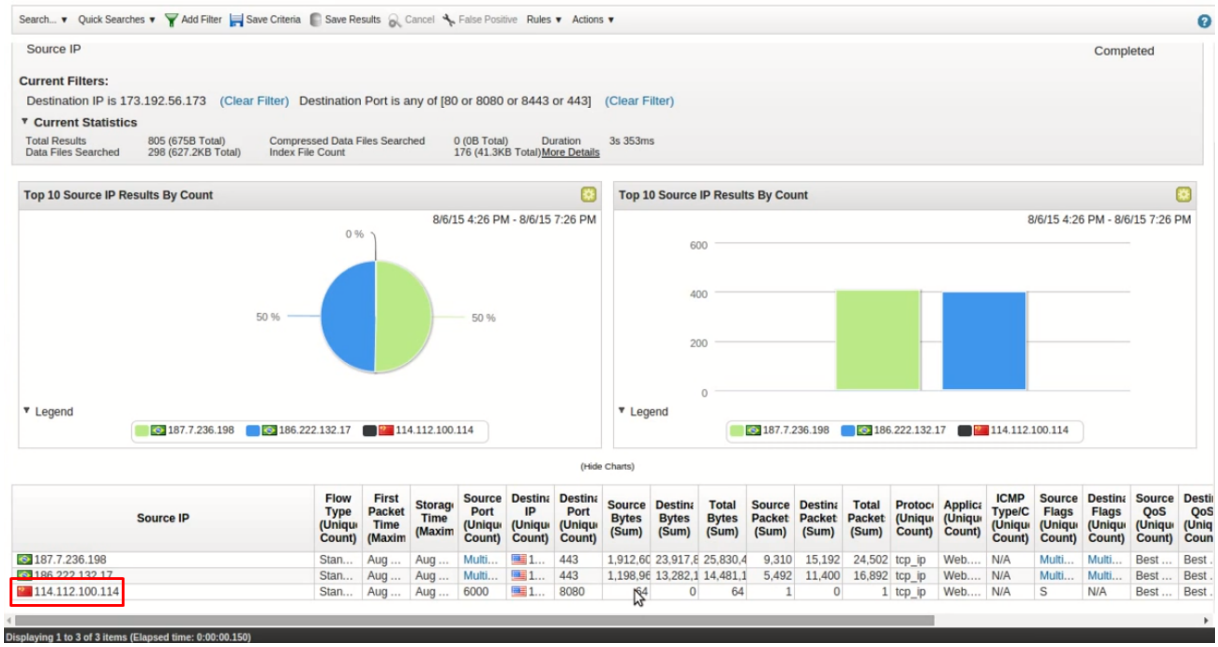
Figura 8 - Identificação do IP do servidor WEB



Fonte: Vídeo Youtube: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s

Após o clique no hiperlink gerado na aba Services IP é possível identificar as tentativas de acesso de cada IP, sendo possível visualizar um IP considerado anormal, que possivelmente é um atacante tentando fazer um ataque de força bruta de login inválido, exemplo na Figura 9.

Figura 9 - Identificação das tentativas de acesso de cada IP



Fonte: Vídeo Youtube: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s

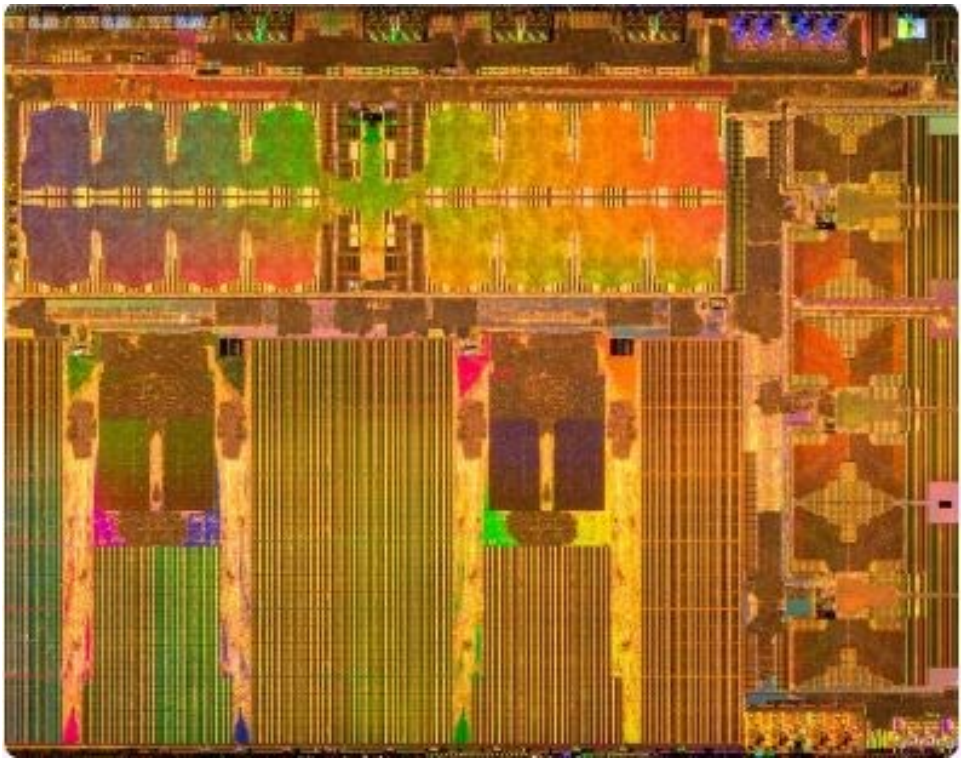
Depois de identificado, basta classificar na ferramenta. O IP chinês é observado como uma possível ameaça, após isso, define-se o diagnóstico do problema de lentidão no servidor WEB.

4.2 Piloto Automático Tesla

A Tesla desenvolve carros que utilizam a Inteligência Artificial, acreditando que com um bom planejamento, uma boa visão avançada dessa tecnologia, e com uma boa eficiência do Hardware, são maneiras de alcançar uma solução geral para autogestão.

Na Figura 10 é possível verificar a construção do Hardware. Por ele se constrói chips de silício que fazem com que impulsione o software autônomo do zero, procurando realizar melhorias arquitetônicas e micro arquitetônicas, para se ter o melhor desempenho de silício por watt. Realizando o planejamento adequado, boas análises do tempo e potência do projeto, é possível criar grandes testes visando a funcionalidade e desempenho, propondo a realização de testes para implementação de compiladores e drivers para se programar e comunicar com o chip. Tendo em vista o foco na otimização do desempenho e a economia da energia. Por fim, a empresa valida o chip de silício e o leva para produção em grande quantidade (TESLA, 2021).

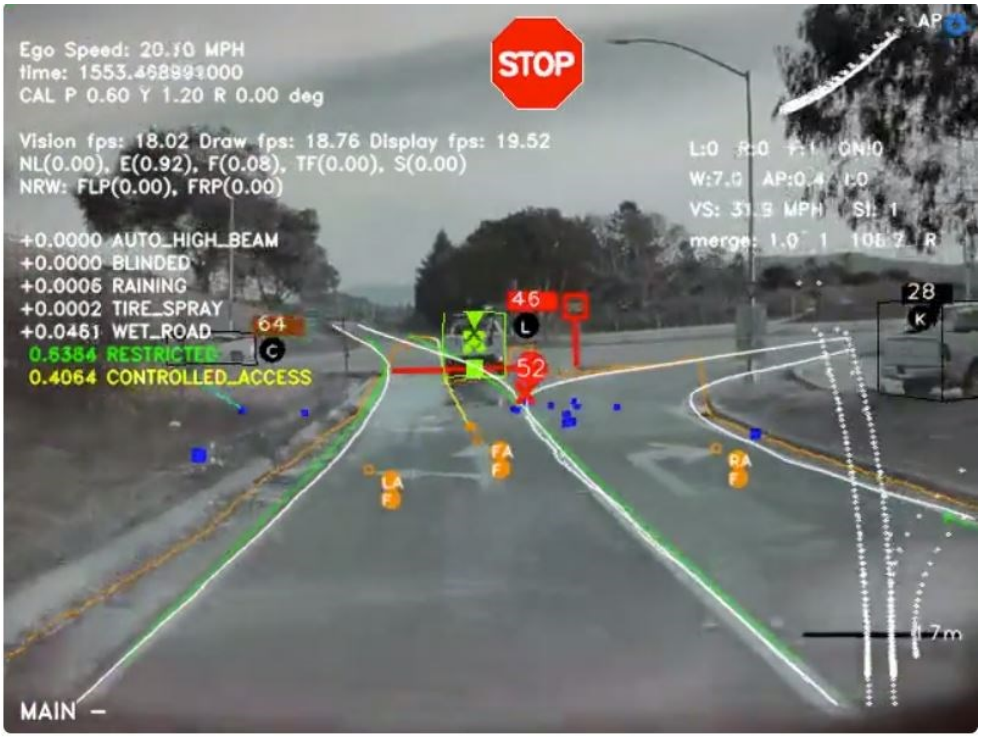
Figura 10 - A construção do Hardware



Fonte: https://www.tesla.com/autopilotAI

A empresa realiza pesquisas de ponta para treinar redes neurais em alguns problemas, podendo ir da percepção ao controle. As redes de câmeras podem analisar imagens para realizar uma detecção dos objetivos com uma análise mais profunda. A Tesla possui redes de visão aérea e reproduzem vídeo de todas as câmeras, para assim ser produzido o layout da estrada, da infraestrutura e objetos 3D, proporcionando vários níveis de visualização, exemplo na Figura 11. As redes neurais aprendem com cenários complicados e diversificados do mundo, e possuem mais de 1 milhão de veículos em tempo real. A construção completa de redes neurais do piloto automático possui 48 redes que podem levar 70.000 horas de GPU (Unidade de Processamento de dados) para serem treinados. Todos juntos geram 1.000 previsões em cada etapa de tempo (TESLA, 2021).

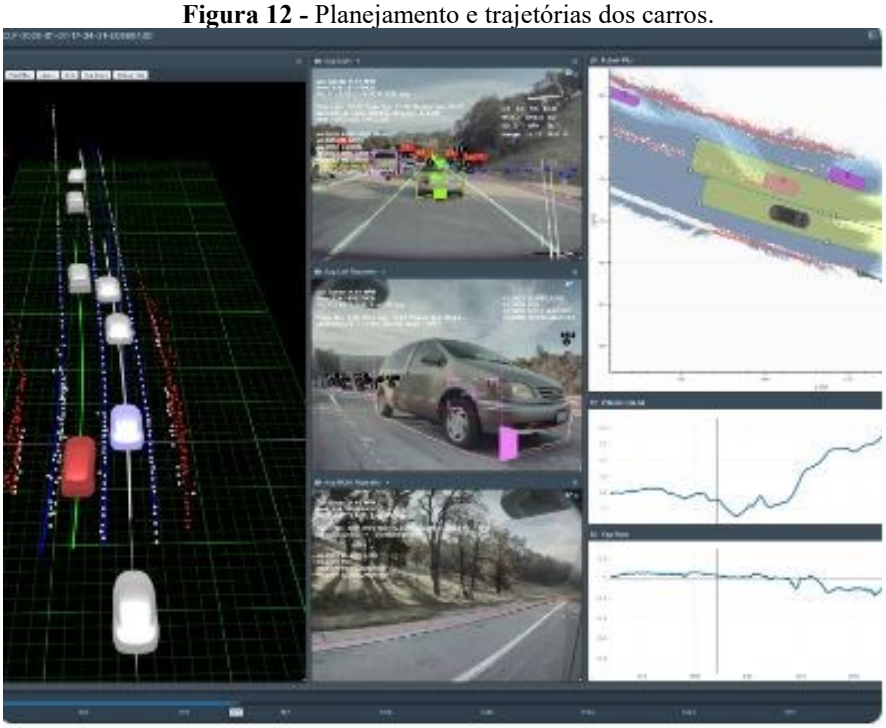
Figura 11 - Estrada com carros em movimento (Redes Neurais)



Fonte: https://www.tesla.com/autopilotAI

A Tesla trabalha com algoritmos que dirigem o carro, representando uma alta fidelidade do mundo e o planejamento de trajetórias, como na Figura 12. Tem a finalidade de treinar as redes neurais para prever representações, e criar algoritmos precisos. Combinando grandes informações dos sensores do carro no tempo e espaço. Utilizam técnicas com tecnologias mais recentes para construção de um sistema robusto, com uma grande precisão na tomada de decisão, que possa trabalhar em situações complicadas no mundo real, podendo enfrentar incertezas (TESLA, 2021).

Figura 12 - Planejamento e trajetórias dos carros.



Fonte: https://www.tesla.com/autopilotAI

Os códigos são implementados verificando sempre a taxa de transferência e latência. São realizadas correções do código caso seja encontrado algum erro, que tem por objetivo otimizar e melhorar a codificação. A construção das bases do software do Piloto Automático é realizada a partir de níveis mais baixos da pilha, realizando a integração com perfeição no hardware personalizado. O carregamento de boot é altamente confiável, e possui suporte para atualizações, podendo criar *kernels* Linux personalizados. O código é escrito tendo uso eficiente da memória para poder capturar dados de alta frequência, e volume dos sensores para poder compartilhar com vários processos do consumidor. Assim, não afetando a latência da memória, e não prejudicando os ciclos da CPU. A computação tem uma variedade de unidades de processamento de hardware, sendo distribuídas em vários sistemas em chips. Já com a infraestrutura de avaliação implementados nas análises, cria-se ferramentas para melhorar a avaliação de hardware, visando acelerar o ritmo da inovação, propondo melhorias no desempenho para evitar retrocessos através de testes automatizados (TESLA, 2021).

4.3 Aplicações de reconhecimento Facial

Um método de ajudar na detecção de uma pessoa que cometeu um crime, pode ser facilitado com o uso do aprendizado de máquina. Dependendo do tipo de algoritmo

implementado de aprendizagem, pode ser útil para identificação através do reconhecimento facial.

Os tipos de algoritmos que podem ser utilizados, têm o objetivo de repetir ações do cérebro humano, que tem o intuito de ajudar em possíveis identificações de objetos como: carros, estradas ou pessoas.

Para utilizar o exemplo de aprendizado de máquina com o reconhecimento fácil, é possível que ela identifique cada traço do rosto, formato, nariz, boca, ou algum traço marcante que faz com que o mesmo seja reconhecido através da I.A. Isso faz com que seja muito útil para um caso de polícia, que ajuda na identificação e consiga diferenciar rostos, que podem ser de pessoas apontadas como responsáveis por tal ato.

Quando ocorre um assalto em uma loja, o departamento policial responsável utiliza as imagens juntamente com a I.A para identificação dos rostos de assaltantes. Os dados das imagens são comparados com os dados de uma fotografia, e com isso é possível verificar se as evidências têm alguma correspondência (HURWITZ E KIRSCH, 2018).

Alguns ambientes de negócios necessitam de um local altamente seguro para o trabalho, e regras que precisam ser seguidas. Sendo assim, aplicações de I.A são altamente eficazes e seguras nesses ambientes.

Conforme o cliente informa quais são as regras que precisam ser executadas pelas aplicações, as câmeras são preparadas a identificarem situações do ambiente, como exemplo: quantas pessoas estão na sala, qual o horário que se pode frequentar o ambiente, entre outras informações que a I.A pode fornecer.

A empresa Gryfo desenvolve aplicações inteligentes. Se regras forem descumpridas, a aplicação envia um alerta para o responsável pelo ambiente, para que a pessoa possa agir o mais rápido possível, para assim evitar grandes perdas para organização e possivelmente se perder a integridade e reputação da empresa. As aplicações desenvolvidas podem também ajudar na detecção de pessoas e no reconhecimento facial, para ajudar a identificar quem está frequentando o ambiente.

Se uma câmera de segurança não utilizar aplicações de I.A, a mesma não terá utilidade alguma, pois serão apenas imagens, e não será possível ter informações mais precisas para se tomar decisões para prevenção de riscos ao ambiente. Ela permite analisar o ambiente como um todo, a frequência que cada pessoa passa pelo local é identificada, e comportamentos suspeitos podem gerar alertas, que podem ajudar na identificação de algum possível crime ou infração.

Também é possível controlar o acesso de pessoas ou veículos em diferentes situações, mas deve-se realizar o processo dos ensinamentos dessas aplicações cuidadosamente para evitar falhas, pois pode ocorrer.

Outra aplicação de I.A desenvolvida pela Gryfo, é adaptada a um hardware, podendo ser uma catraca por exemplo. Essa aplicação permite controlar o acesso de pessoas com certa rapidez, evitando assim fraudes ou ataques utilizados pela engenharia social.

Somente com o uso dessa tecnologia é liberado o acesso a pessoas, através do reconhecimento facial, assim somente pessoas que estão cadastradas nos sistemas, e estão autorizadas para estarem ali, tem o seu acesso liberado. Ela permite também identificar o movimento, somente com a pessoa olhando para a câmera para seu acesso ser liberado.

A Inteligência Artificial pode ser aplicada de muitas maneiras diferentes, e o negócio sempre estará mais seguro com a sua utilização. O investimento dessa tecnologia vem para trazer cada vez mais segurança a todos os ambientes (GOMES, 2020).

5 CONSIDERAÇÕES FINAIS

A Segurança da Informação é um fator importante para garantir a integridade, confidencialidade, disponibilidade e autenticidade da empresa. A empresa que investe corretamente na Segurança da Informação possui um menor risco de sofrer com vulnerabilidades, que acarretam a perda de dados que podem fazer com que a mesma perca dinheiro e coloque em risco os ativos da organização, assim como sua confiança com clientes e parceiros. A Segurança necessita do uso de tecnologias, assim como da preparação adequada de pessoas. Exige que se conheça principalmente a organização e o negócio acima dos riscos e das ameaças, pois o motivo de existir a Segurança da Informação é o próprio negócio. Procura-se minimizar os riscos existentes, e realizar o investimento adequado de aplicações eficientes é indispensável.

A Inteligência Artificial está presente em várias áreas da tecnologia, inclusive na área da Segurança da Informação. Nos dias atuais vem surgindo cada vez mais ferramentas e aplicações que utilizam essas máquinas inteligentes. A interação do ser humano com essas máquinas ajuda em atividades do cotidiano, fazendo com que atividades antes desenvolvidas pelos humanos, passem a serem realizadas de forma automática, podendo assim aumentar a produtividade dos profissionais que podem se dedicar a outras tarefas mais complexas. Isso se torna uma vantagem para as empresas que investem nessas aplicações de I.A. Ferramentas que possuem essa tecnologia podem ser utilizadas para defender o negócio da organização.

Os profissionais da área de segurança estão sempre se dedicando para acompanhar os meios utilizados pelos atacantes, e os sistemas de I.A podem prover um auxílio a curto prazo. Aumentando significativamente a variação dos mecanismos de defesa. A automação de parte das tarefas, auxiliam a preencher a falta de mão de obra e aumenta a eficiência dos profissionais. Mas, a utilização da I.A também podem trazer alguns riscos. Algumas ações ou codificações não ensinadas corretamente para máquina, podem fazer com que a mesma tome decisões equivocadas que possam trazer um risco na segurança. A falta de inteligência emocional da máquina, podem gerar questionamentos em tomadas de decisão que envolvem aspectos éticos.

Esses profissionais que treinam as máquinas precisarão passar por essas dificuldades, e treinar as máquinas melhorando sempre suas codificações e entendimento. Esses métodos de codificações inteligentes podem aprimorar cada vez mais os conhecimentos, com a combinação adequada da Inteligência Humana e Inteligência Artificial. A Inteligência Artificial não vem para substituir profissionais adequados e qualificados com conhecimentos técnicos necessários. Esses profissionais de segurança devem trabalhar junto com a Inteligência Artificial e suas

tecnologias, equilibrando a supervisão humana e fornecendo a confiança necessária para que a I.A possa atuar de forma autônoma e eficaz.

REFERÊNCIAS

CHAN; SIMON; MIN*; at al*. ***Survey of AI in Cybersecurity for Information Technology Management.*** Europa: IEEE Technology & Engineering Management Conference (TEMSCON), 2019.

GOMES, V. **5 Aplicações de Inteligência Artificial em câmeras de segurança.** São Paulo: Gryfo, 2020. Disponível em: https://gryfo.com.br/blog/2020/05/22/5-aplicacoes-inteligencia-artificial-gryfo. Acesso em: 7 jun. 2021.

GUTIERREZ, A. **É possível confiar em um sistema de inteligência artificial?** Práticas em torno da melhoria da sua confiança, segurança e evidências. São Paulo: Revista dos Tribunais, 2019.

HURWITZ, J.; KIRSCH, D. ***Machine Learning***. United States: IBM Limited Edition, 2018.

IBM**. Data Responsibility.** Estados Unidos: 2017. Disponível em: https://www.ibm.com/blogs/policy/wp-content/uploads/2017/10/IBM_DataResponsibility-USLetter_WEB.pdf. Acesso em: 3 nov. 2020.

IBM. ***IBM QRadar SIEM***. New York: IBM, 2021. Disponível em: https://www.ibm.com/br-pt/products/qradar-siem. Acesso em: 26 jan. 2021.

IBM. **Inteligência artificial para um tipo de segurança cibernética mais inteligente.** New York: IBM, 2020. Disponível em: https://www.ibm.com/br-pt/security/artificial-inte.lligence?p1=Search&p4=43700052743495189&p5=b&cm_mmc=Search_Google-_-1S_1S-_-LA_BR-_-%2Bseguran%C3%A7a%20%2Bintelig%C3%AAncia%20%2Bartificial_b&cm_mmca7=71700000065214064&cm_mmca8=kwd-892642482602&cm_mmca9=CjwKCAjw_Y_8BRBiEiwA5MCBJsvVi7K1n9ANN4txwCCE02--ZO1h1zLOL_XtSBZPgNcCsQ5VPxYwrRoC04wQAvD_BwE&cm_mmca10=428258351718&cm_mmca11=b&gclsrc=aw.ds&&gclid=CjwKCAjw_Y_8BRBiEiwA5MCBJsvVi7K1n9ANN4txwCCE02--ZO1h1zLOL_XtSBZPgNcCsQ5VPxYwrRoC04wQAvD_BwE. Acesso em: 01 set. 2020.

IBM. ***Machine Learning*** **e Ciência de dados com IBM Watson**. New York: IBM, 2020. Disponível em: https://www.ibm.com/br-pt/analytics/machine-learning. Acesso em: 25 set. 2020.

MACHADO, V. P. **Inteligência Artificial**. Piauí: Universidade Federal do Piauí, 2020. Disponível em: http://www.uece.br/computacaoead/index.php/downloads/doc_download/2177-inteligencia-artificial. Acesso em 14 set. 2020.

MUNDO MAIS TECH**. Qual o impacto da Inteligência Artificial na segurança dos dados?** Rio de Janeiro: Embratel, 2020. Disponível em: https://mundomaistech.com.br/inteligencia-artificial/qual-o-impacto-da-inteligencia-artificial-na-seguranca-dos-dados/. Acesso em: 20 set. 2020.

NORVIG, P.; RUSSEL, S. **Inteligência Artificial**. Rio de Janeiro: Elsevier Editora, 2013.

OLIVEIRA, W. **Princípios Básicos da Segurança da Informação.** São Paulo: TechTem, 2021. Disponível em: https://www.techtem.com.br/principios-basicos-da-seguranca-da-informacao. Acesso em: 20 abr. 2021

PINTO, H. A. **A utilização da inteligência artificial no processo de tomada de decisões**. Brasília: Revista da informação legislativa, 2020.

RANGERS, H. **Caso prático de uso do IBM QRadar – Análise de Flow de Rede**. 2015. (7m27s). Disponível em: https://www.youtube.com/watch?v=FY2gXGwE35A&t=232s. Acesso em: 26 jan. 2021.

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. São Paulo: Pearson Education do Brasil, 2014.

STEFANINI. **As 7 principais aplicações de Inteligência Artificial nas empresas.** Brasil: Stefanini Brasil, 2020. Disponível em: https://stefanini.com/pt-br/trends/artigos/as-7-principais-aplicacoes-de-inteligencia-artificial-nas-empres. Acesso em: 15 nov. 2020.

TESLA. **Autopilot.** California: Tesla, 2021. Disponível em: https://www.tesla.com/autopilotAI. Acesso em: 15 mai. 2021.

TIMOCHENCO, L. **Inteligência Artificial na Segurança da Informação.** São Paulo: Revista Digital Online, 2020. Disponível em: https://infranewstelecom.com.br/inteligencia-artificial-na-seguranca-da-informacao. Acesso em: 25 out. 2020.

TURING, A. M. **Computing Machinery and Intelligence.** Reino Unido: Oxford University Press on behalf of the Mind Association, 1950.