# Propósito e Objetivos


O propósito da Cybersecurity na camada de New Technology é robustecer a proteção contra ataques digitais, garantindo a segurança dos dados sensíveis e a resiliência dos sistemas de TI.

A integração da Inteligência Artificial (AI) em estratégias de segurança cibernética representa um avanço significativo, permitindo respostas mais ágeis e inteligentes a

ameaças em evolução constante.

Objetivos da Cybersecurity integrada com AI:

· Detecção de Ameaças Melhorada: Utilizar algoritmos de AI para monitorar, detectar e analisar atividades suspeitas em tempo real, identificando ameaças potenciais com maior precisão.

· Resposta a Incidentes Acelerada: Desenvolver sistemas capazes de responder automaticamente a incidentes de segurança, reduzindo o tempo de reação e mitigando os danos potenciais.

· Automatização de Tarefas de Segurança: Implementar processos automatizados para atualizações de segurança e patches, diminuindo a carga operacional sobre as equipes de TI.

· Análise Preditiva de Segurança: Empregar modelos preditivos para prever e se preparar para ataques cibernéticos futuros, fortalecendo as defesas antes de qualquer comprometimento.

· Adaptação e Aprendizado Contínuo: Assegurar que os sistemas de segurança possam aprender com ataques anteriores e adaptar suas estratégias para enfrentar novos vetores de ataque.

· Inteligência Contra Ameaças: Colaborar na criação e no compartilhamento de inteligência sobre ameaças, aproveitando o conhecimento coletivo para melhorar a proteção.

· Governança e Conformidade: Reforçar políticas e procedimentos de segurança para garantir conformidade com regulamentos e padrões da indústria.

· Educação e Conscientização: Promover a conscientização sobre cybersecurity em todos os níveis organizacionais, utilizando AI para personalizar treinamentos e simulações de segurança.

· Desenvolvimento de Talentos: Investir na formação e capacitação de profissionais de segurança em tecnologias emergentes e técnicas avançadas de AI.

· Segurança como Cultura Organizacional: Integrar práticas de segurança cibernética como um elemento fundamental da cultura organizacional.

· Parcerias Estratégicas: Estabelecer parcerias com fornecedores de tecnologia, instituições acadêmicas e organizações governamentais para desenvolver soluções inovadoras em cybersecurity.

· Proteção de Infraestruturas Críticas: Aplicar AI para proteger infraestruturas críticas e sistemas de controle industrial contra ataques sofisticados.

· Análise Comportamental: Utilizar análise comportamental avançada para identificar desvios e prevenir ameaças internas.

Ao abraçar a AI como um componente crítico na estratégia de cybersecurity, as organizações podem não apenas reforçar suas defesas contra agentes maliciosos, mas também avançar em direção a uma postura proativa, onde antecipar e neutralizar riscos se torna parte integrante do ecossistema tecnológico.