KPIs Usuais

A cibersegurança é uma área de importância crescente, especialmente com a integração cada vez maior da Inteligência Artificial (AI) em sistemas de segurança.

Esta integração não só potencializa as capacidades de proteção e resposta como

também eleva a complexidade e a sofisticação necessárias para prevenir e combater ameaças digitais avançadas.

Com a IA se tornando uma ferramenta tanto para defensores quanto para adversários, os KPIs (Key Performance Indicators) no âmbito da cibersegurança devem refletir tanto o desempenho das soluções de segurança quanto a preparação contra ameaças baseadas em IA.

Dentro deste contexto, os KPIs considerados cruciais para a gestão de cibersegurança incluem:

· Taxa de Detecção de Intrusão: A eficácia dos sistemas em identificar tentativas de acesso não autorizado.

· Tempo Médio para Detectar (MTTD): O tempo que leva para identificar uma brecha de segurança desde o momento de sua ocorrência.

· Tempo Médio para Responder (MTTR): A rapidez com que a equipe de segurança consegue responder a uma ameaça identificada.

· Número de Incidentes de Segurança: A quantidade de eventos de segurança que ocorrem dentro de um determinado período.

· Taxa de Falsos Positivos e Falsos Negativos: A precisão dos sistemas de IA em diferenciar entre atividades legítimas e maliciosas.

· Efetividade da Resposta a Incidentes: Avalia a adequação e a eficácia das ações tomadas após a detecção de um incidente.

· Taxa de Sucesso de Recuperação: A capacidade de restaurar sistemas e dados após uma violação de segurança.

· Custo Médio de um Incidente de Segurança: O impacto financeiro total de um incidente de segurança, incluindo remediação e perda de reputação.

· Percentual de Cobertura de Auditoria: A proporção de sistemas e aplicativos regularmente auditados por vulnerabilidades.

· Nível de Conformidade com Padrões de Segurança: A aderência da organização às normas de segurança estabelecidas, como ISO 27001, NIST, etc.

· Taxa de Atualização de Patches: A rapidez e a consistência com que as atualizações

de segurança são aplicadas.

· Avaliação de Risco de Terceiros: A segurança dos sistemas relacionados a fornecedores e parceiros.

· Capacidade de Detecção de Anomalias Baseada em AI: A habilidade dos sistemas alimentados por IA de identificar comportamentos atípicos que possam indicar ameaças.

· Maturidade do Modelo de Segurança: A evolução do modelo de segurança da organização, incluindo a integração de AI para defesa e resposta.

· Engajamento em Treinamento e Conscientização: A frequência e a eficácia dos programas de treinamento de segurança para funcionários.

Esses indicadores são essenciais para medir a eficácia das estratégias de cibersegurança e devem ser continuamente revisados e adaptados à medida que novas tecnologias e métodos de ataque surgem.

A incorporação de IA em sistemas de cibersegurança é uma tendência que está definindo novos paradigmas na proteção de ativos digitais, exigindo que as organizações estejam preparadas para enfrentar ameaças cada vez mais sofisticadas.

The IT framework