1.*Threat Intelligence*

Os profissionais de segurança de TI precisam estar sempre atualizados sobre as ameaças mais recentes que podem afetar suas organizações. Além de conhecer as ameaças, é fundamental entender os agentes responsáveis por elas, pois isso pode indicar a origem de um ataque. Felizmente, há uma grande quantidade de informações disponíveis na internet sobre grupos de hackers e as ferramentas que utilizam para atacar redes. Com base nessas informações, as decisões de segurança podem ser mais bem fundamentadas, permitindo a escolha de ferramentas e estratégias adequadas para defesa.

A inteligência sobre ameaças pode ser útil para diversos setores dentro da organização. Pesquisadores podem utilizá-la para compreender melhor os riscos, enquanto equipes de TI podem empregá-la para fortalecer a proteção contra ataques. Um dos principais recursos de inteligência de ameaças é a **OSINT** (Open-Source Intelligence), que consiste em informações públicas disponíveis para qualquer pessoa que saiba onde procurar. Na internet, grupos de discussão, redes sociais e publicações de pesquisadores podem fornecer insights valiosos. Além disso, o governo disponibiliza uma vasta quantidade de informações em audiências públicas, relatórios e sites institucionais.

Empresas privadas também disponibilizam dados comerciais relevantes, como relatórios financeiros e bancos de dados sobre projetos e riscos organizacionais. Algumas empresas especializadas reúnem e analisam essas informações, oferecendo inteligência de ameaças como um serviço pago. O diferencial dessas organizações é a capacidade de monitorar ameaças em diversas empresas simultaneamente. Ao identificar padrões de ataque em uma determinada área, elas podem alertar outras organizações antes que sejam afetadas.

A colaboração entre empresas é outro fator essencial na cibersegurança. Iniciativas como a **Cyber Threat Alliance (CTA) permitem que organizações compartilhem informações sobre ameaças em um formato padronizado**, atribuindo níveis de severidade a cada uma delas. Isso possibilita que todos os membros da aliança tenham acesso a dados atualizados e possam tomar decisões estratégicas de defesa.

Uma fonte de inteligência de ameaças ainda mais detalhada é a dark web, uma camada da internet acessível apenas com softwares especializados. Nesse ambiente, é possível encontrar grupos de hackers discutindo suas atividades, ferramentas utilizadas e até mesmo vendendo dados roubados, como informações de cartões de crédito. Monitorar esses fóruns pode ser crucial para detectar possíveis ataques direcionados à organização.

Dessa forma, manter-se informado sobre ameaças e compartilhar informações com outras empresas são estratégias essenciais para uma defesa eficaz no ambiente digital.