Cyber Threat Intelligence: o novo aliado da Cibersegurança

dinheirovivo.pt/opiniao/cyber-threat-intelligence-o-novo-aliado-da-ciberseguranca-16915536.html

29 de agosto de 2023

No decorrer dos últimos três anos, começou a ser evidente o impacto do uso das competências de "intelligence" contra as ameaças cibernéticas oriundas do mundo cibercriminoso, que vai desde o fornecimento de informações para a tomada de decisões em violentos ataques de ransomware até aos conflitos cibernéticos da Guerra da Ucrânia, revelando-se um grande aliado no setor da cibersegurança a nível mundial. Devemos, então, perceber, como é que a Cyber Threat Intelligence (CTI) auxilia a defesa contra as ameaças cibernéticas?

Relacionados

Quando o cibercrime não tira férias: 8 dicas para se manter em (ciber)segurança

Presidência espanhola do Conselho da UE: uma aposta promissora na inteligência artificial e na cibersegurança

A CTI começa sempre o seu ciclo de trabalhos por planear e orientar na preparação da sua equipa; e justamente, uma das atividades cruciais nesta primeira fase é a definição de requisitos de informação e prioridades do seu trabalho no contexto de uma organização. Tal como os requisitos são parte fundamental para as questões problemáticas da organização, as fontes de informação também são vitais para a qualidade e precisão da ação da CTI, podendo estas ser fontes externas, como feeds de ameaças comerciais ou de fonte aberta, notícias, monitorização de canais de comunicação na darkweb, etc., ou fontes internas como, por exemplo, o registo de eventos de segurança e dados forenses no seguimento de um ciberataque. No que se

refere à produção e consumo, várias organizações começam por analisar os seus próprios dados sobre violações de dados ou intrusões de rede e produzem através dessa informação produtos de intelligence (relatórios); contudo, também podem gerar dados em bruto, por exemplo, listas de IOC"s (indicadores de compromisso). Para auxiliar a CTI a produzir e a consumir informação de qualidade surgem diversas ferramentas que auxiliam no caminho rumo ao sucesso e eficiência; contudo, o mais relevante é efetivamente a experiência dos analistas e a metodologia aplicada (vezes sem conta) na angariação e processamento de informação. Outra etapa essencial são os processos analíticos, e nesta fase, o que temos observado é a utilização de métodos como a análise intuitiva, a modelação de ameaças e a utilização de modelos conceptuais, apesar do método mais utilizado ser a análise intuitiva. Ainda assim, é importante frisar que sustentam essa análise com modelos conceptuais, técnicas analíticas estruturadas (SAT) e gráficos, para que a análise não seja incorreta. O ciclo da CTI finaliza quando se procede à divulgação da informação, existindo

sempre uma preocupação para que a informação produzida chegue às pessoas ou sistemas certos, no momento preciso, para poderem utilizar a mesma da melhor forma e em tempo útil.

Por ser uma área tão recente, enfrenta ainda vários desafios e limitações que muitas vezes podem impedir a CTI de avançar e evoluir, sendo apontados como principais motivos: a falta de formação, a falta de recursos humanos especializados, a falta de tempo e ainda a falta de automatização num processo que envolve sempre "big data" em formato "cru". Outro grande desafio tem sido a dificuldade crescente que os analistas de CTI enfrentam devido ao volume crescente de feeds de informação de fonte aberta. Estes feeds de informação com a subsequente necessidade de responder às diversas questões que os mesmos levantam, nomeadamente, a credibilidade das fontes ou a capacidade de ser atempadamente identificadas, é uma área em que o domínio da CTI poderia beneficiar de melhores práticas e processos adicionais, para minimizar o risco da desinformação. O enviar informação desatualizada ou incorreta coloca rapidamente em causa a credibilidade do serviço da CTI.

Os acontecimentos mundiais vão continuar a exercer influência sobre a CTI, seja sob a forma de conflitos geopolíticos ou do aparecimento de novo malware. A CTI continuará a ser uma força (cada vez mais) potente para orientar as equipas a combater as ciberameaças e auxiliar na maior capacitação das partes interessadas, de todos os tipos, na tomada estratégica de decisões. À medida que esta vertente continua a evoluir, esperamos assistir a uma maturidade consistente, enquanto o mundo moderno enfrenta novos desafios e abordam áreas emergentes nesta nova era da informação.

Quando o aumento dos ciberataques continua na ordem do dia e no radar dos meios de comunicação social e da camada de gestão de topo das organizações, importa realçar que, cada vez mais, existem novas ferramentas, recursos e soluções que ajudam à

definição da estratégia de segurança, e que a CTI poderá ser a chave para evitar ou minimizar os danos de um ciberataque mesmo quando desenvolvido por grupos cibercriminosos altamente evoluídos. Façamos então bom uso deste "novo" aliado no mundo da prevenção ao cibercrime.

Bruno Castro, fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense.