01 / OBJETIVO E INVESTIMENTO

Próxima etapa
Perfilamento de ameaças

Cashfast e Zaztech | Cyber Threat Intelligence (CTI) e investigação técnica de padrões de ataque.

R$ 30.000 a R$ 60.000

Faixa indicativa para um projeto pontual. Prazo preliminar: 15 a 30 dias úteis após a definição do escopo e o atendimento dos pré-requisitos.

O que é perfilamento

É uma investigação técnica orientada por evidências para caracterizar padrões de atividade hostil, relacionar eventos e campanhas e compreender as táticas, técnicas e procedimentos observáveis. O foco é transformar telemetria em inteligência acionável para fortalecer detecção, triagem e prevenção.

Por que após o White Box

Os pentests revelarão os fluxos críticos, superfícies de aplicação, controles e lacunas de observabilidade. Essa base permitirá identificar quais fontes de dados são relevantes, quais eventos precisam ser registrados e quais hipóteses podem ser investigadas com evidência suficiente.

Condição da estimativa

A faixa de R$ 30.000 a R$ 60.000 não é um orçamento fechado. O valor depende diretamente dos achados do White Box, da disponibilidade, qualidade, retenção e volumetria dos logs, da quantidade de ambientes autorizados, do período de análise e da complexidade dos cenários. Poderá ser revisado para mais ou para menos mediante dimensionamento técnico.

Escopo, prazo, preço final e condições de pagamento serão formalizados em proposta específica. A etapa é opcional e independente dos R$ 80.000 da contratação conjunta dos pentests e do respectivo desconto de R$ 50.000.

02 / METODOLOGIA

Como a investigação é conduzida

01. Discovery e qualificação das evidências

Definir objetivos, empresas e ambientes autorizados, período de análise e fontes disponíveis. Avaliar cobertura e retenção de logs, granularidade, sincronização temporal, permissões e lacunas. Estabelecer critérios de suficiência e priorizar hipóteses a partir do White Box.

02. Preparação e correlação da telemetria

Receber exportações autorizadas ou acessos de leitura. Normalizar eventos, horários, identificadores e campos relevantes; tratar duplicidades e dados sensíveis. Correlacionar registros de aplicações, APIs, AWS, Cloudflare e demais fontes aprovadas.

03. Identificação de padrões e campanhas

Analisar recorrência temporal, classes de eventos, padrões de requisição, tentativas de acesso, alvos e comportamentos observáveis. Agrupar eventos por similaridade e contexto, distinguindo sinais de automação, possíveis campanhas e atividade legítima.

04. Caracterização das ameaças

Registrar indicadores de comprometimento (IOCs), quando sustentados por evidências, e mapear táticas, técnicas e procedimentos (TTPs) para MITRE ATT&CK quando aplicável. Documentar hipóteses alternativas, evidências contrárias, limitações e nível de confiança.

05. Recomendações e entrega

Consolidar linha do tempo, padrões, hipóteses, indicadores e lacunas. Recomendar fontes e campos de log, regras de detecção e critérios de triagem; apresentar as conclusões e prioridades à equipe responsável.

Fontes previstas, mediante autorização

Logs de aplicação e API, autenticação e autorização, eventos de WAF/Cloudflare, trilhas de auditoria de nuvem (AWS), registros de segurança e evidências do White Box. A coleta será limitada ao necessário e às fontes disponibilizadas pelo cliente.

03 / ENTREGÁVEIS E LIMITES

Inteligência acionável, com limites claros

Entregáveis previstos

- Relatório técnico com metodologia, fontes, período, cobertura, lacunas, linha do tempo e conclusões.
- Matriz de padrões e hipóteses de campanhas, IOCs e TTPs aplicáveis, com evidências e níveis de confiança.
- Recomendações priorizadas de instrumentação, regras de detecção, triagem e melhoria da observabilidade.
- Apresentação dos resultados e discussão das prioridades com as equipes técnicas.

Premissas e proteção das informações

A investigação exige autorização formal, pontos focais, telemetria suficiente e acesso limitado às fontes aprovadas. O tratamento de evidências observará o NDA, a minimização de dados, a segregação por empresa, o controle de acesso e as regras de retenção e descarte acordadas. Lacunas ou baixa confiabilidade poderão limitar as conclusões e alterar o dimensionamento.

O que não está incluído

- Identificação garantida de pessoas físicas, atribuição conclusiva de autoria, investigação jurídica, medidas legais ou perícia judicial.
- Monitoramento contínuo, SOC 24×7, resposta a incidentes, coleta invasiva ou testes contra sistemas de terceiros.
- Implementação de controles, instrumentação, regras de detecção, remediação ou novos pentests; essas atividades exigem contratação específica.

Próximos passos

Concluir o White Box; revisar os achados e lacunas de telemetria; realizar discovery de dimensionamento; confirmar abrangência, critérios de aceite, prazo e investimento em proposta separada. Não há obrigação de contratação desta etapa.