REGULAMENTO DO CHALLENGE TECNOLÓGICO "Hackathon Challenge de Ciber Segurança" da ALIANÇA PORTUGUESA DE BLOCKCHAIN

I. Definição do Desafio

1. O desafio **Hackathon Challenge de Ciber Segurança** é uma iniciativa desenvolvida em parceria pelo ISEC (Instituto Superior de Engenharia de Coimbra) e a Aliança Portuguesa de Blockchain (APB), devidamente enquadrada nos objetivos traçados pela Aliança, que passam pela promoção do conhecimento sobre tecnologias exponenciais e pelo incentivo ao desenvolvimento de soluções inovadoras baseadas nestas tecnologias.
2. O ISEC será a entidade apadrinhadora deste desafio, cuja organização caberá à Aliança Portuguesa de Blockchain.
3. O Hackathon Challenge de Ciber Segurança tem como base o seguinte desafio: **como podemos desenvolver uma solução de Ciber Segurança que automaticamente classifique, e preveja a vulnerabilidade de determinadas entidades (indivíduos, empresas, agências e países) para apoiar essas entidades a lidar com os seus níveis de vulnerabilidade (baixo, medio, alto, extremo, etc.)**. Através deste desafio pretendemos receber soluções que alavanquem os *"datasets"* disponíveis (Ver anexo) de forma a permitir a identificação de "ameaças", construção de ferramentas e serviços que alertem as entidades das suas vulnerabilidades, criação de soluções que recomendem qualquer entidade sobre a proteção contra um Ciber Ataque, e a monetização da solução para distribuição e gestão das múltiplas entidades alertadas.

II. Objetivo do Desafio

1. O **Hackathon Challenge de Ciber Segurança** tem como objetivo:
    a) Promover a inovação no âmbito da Ciber Segurança no tecido empresarial português;

III. Destinatários do Desafio

1. O **Hackathon Challenge DE Ciber Segurança** dirige-se a duas categorias de participantes:
    a) Startups;
    b) Estudantes.

Devem-se sempre candidatar grupos de 2 a 8 pessoas independentemente da categoria do participante (startups ou universidades). Os grupos podem ser compostos por um conjunto de entidades parceiras desde que pertençam à mesma macro categoria: Público ou Privado (exemplo: ou grupo composto por alunos de várias universidades ou grupo composto por duas empresas com competências complementares).

IV. Inscrição e Requisitos

1. Os participantes do **Hackathon Challenge de Ciber Segurança** devem submeter a sua inscrição através do site do Hackathon ou da Aliança (na página disponível em: https://all2bc.com/participar) completando todos os campos obrigatórios, abaixo referidos:
    a) Nome do grupo;
    b) Número de membros do grupo;
    c) Nome completo dos participantes;

d) Idade dos participantes;
e) Email dos participantes;
f) Seleção do *Hackathon Challenge de Ciber Segurança;*

2. Para qualquer questão ou informação adicional sobre o processo de inscrição, deverá ser utilizado o contacto info@all2bc.com

V. Fases e Processo de Seleção do Desafio

1. O **Hackathon Challenge de Ciber Segurança** é composto por três fases:

I. **Desenvolvimento** da solução proposta. A primeira fase (**Desenvolvimento**) centra-se em desenvolver o conceito da solução apresentada. Este desenvolvimento é feito em grupo, será apoiado num espírito de *mentoring* pelo ISEC e Aliança. Deverá ser submetido um documento único limitado a 7 páginas no corpo principal. No mínimo, os seguintes tópicos são obrigatórios:
   - Sumário da Solução;
   - Conceito Final;
   - Benefícios;
   - Anexos.

II. ***Mentoring*** da solução. Após o Desenvolvimento, a candidatura é validada pela entidade promotora do *Hackathon Challenge de Ciber Segurança*, o que inclui um processo de *mentoring*. Esta fase centra-se em melhorar a demonstração da solução. Neste momento, deverá ser submetido um documento/mockup:
   - Um **documento/ mockup de aplicação** com no máximo 10 slides que deverá ser a apresentação a utilizar perante o júri de seleção com, no mínimo, os seguintes tópicos obrigatórios:
     - Sumário Executivo;
     - Abordagem ao *challenge*;
     - Solução Final;
     - Mérito e Evolução da Solução;
     - Potencial de Aplicabilidade;
     - Benefícios;
     - Anexos;

III. **Apresentação** da(s) solução(ões) finalista(s). Por fim, os participantes deverão realizar uma apresentação / demonstração da solução perante o júri de seleção. A apresentação não poderá exceder os 15 minutos. Após esse período, o júri de seleção disporá de um máximo de 5 minutos para colocar questões aos concorrentes.

VI. Prazos do Hackathon e Formatos das Fases de Seleção

Fase I: Desenvolvimento

1. O Hackathon Challenge de Ciber Segurança tem início a 14 de maio de 2019 e o período de submissão de ideias encerra às 15:59 de 14 de maio 2019.
2. Todos os documentos devem ser enviados em formato PDF e com um máximo de 5 Mb;
3. Esta fase continuara até á apresentação final.

4. Em parceria, o ISEC e a Aliança Portuguesa de Blockchain farão a avaliação inicial das ideias recebidas;

Fase II: *Mentoring*

1. A partir das 16:00 do dia 14 de maio, o ISEC e a Aliança Portuguesa de Blockchain farão a avaliação das ideias e darão feedback para melhoria das mesmas;
2. Esta fase continuará até á fase de apresentação.

Fase III: Apresentação

1. As apresentações perante o júri de seleção decorrerão no dia 15 de maio no local do hackathon e horários a designar após as 17h;
2. A ordem das apresentações será estabelecida de forma aleatória;
3. No seguimento das apresentações, o júri irá avaliar as soluções apresentadas e deliberar sobre quais serão consideradas finalistas para apresentar na conferencia do dia seguinte. Até às 23:59 do dia 15 de maio de 2019, os participantes serão informados da decisão do júri. No dia seguinte (16 de maio) as equipas finalistas apresentam na conferência a suas soluções.

São aceites vídeos ou fotografias somente se contextualizados no(s) documento(s) submetido(s). Os vídeos devem estar no Youtube em formato Não Listado e com duração máxima de 2 minutos. As fotografias devem ser em formato JPEG e não ter mais de 1 Mb.

VII. Critérios de Mérito da Solução

Os projetos serão avaliados segundo os seguintes critérios:

- Inovação (25%)
- Impacto no sector (20%)
- Aplicabilidade ao mercado (20%)
- Exequibilidade (15%)
- Escalabilidade (10%)
- Apresentação (10%)

VIII. Júri de Seleção

1. A avaliação do conceito e demonstração cabem ao Júri de Seleção.
2. O Júri de Seleção será composto por elementos das seguintes entidades: ISEC, Aliança Portuguesa de Blockchain, e outros membros a apresentar.
3. A decisão do Júri de Seleção é definitiva e não é passível de recurso

IX. Incentivos

1. Poderão ser entregues incentivos para os melhores projetos por parte da entidade promotora do *Hackathon Challenge de Ciber Segurança*.
2. Os incentivos poderão passar pelas seguintes possibilidades:
   - Comunicação junto dos *media* e parceiros das equipas vencedoras;
   - Estágios profissionais residentes em parceiros da iniciativa;
   - Horas de *Mentoring* com CEOs parceiros da iniciativa;
   - Prémios não pecuniários de participação. (e.g. Drones, Parrots).

X. Proteção de Dados Pessoais

1. Para efeitos da legislação sobre Proteção de Dados Pessoais, informa-se que os dados pessoais fornecidos pelos concorrentes serão objeto de tratamento

automatizado pelo ISEC e pela Aliança Portuguesa de Blockchain, enquanto Responsáveis pelo Tratamento.
2. O tratamento dos dados pessoais dos concorrentes pelo ISEC e pela Aliança Portuguesa de Blockchain tem como finalidades (i) a gestão da sua participação no desafio, (ii) a atribuição de incentivos aos participantes com os melhores projetos e o (iii) cumprimento de obrigações legais. O tratamento dos dados pessoais para as finalidades (i) e (ii) é realizado com base na necessidade de execução deste desafio, no qual os concorrentes participam voluntariamente, sendo que o não fornecimento dos dados pessoais inviabiliza a participação do concorrente no desafio. O tratamento dos dados para a finalidade (iii) constitui uma obrigação legal e é realizado com base na sua necessidade para efeitos de cumprimento de obrigações jurídicas a que o ISEC e a Aliança Portuguesa de Blockchain estão sujeitas.
3. Os dados pessoais tratados para as finalidades (i), (ii) e (iii) serão conservados pelo período de duração do desafio e, para além disso, pelo período estritamente necessário para o cumprimento de obrigações legais.
4. O ISEC e/ou a Aliança Portuguesa de Blockchain poderão contratar terceiros para fornecer suporte de logística ou outro suporte administrativo (por exemplo, partes que fornecem tecnologias de informação). Essas partes podem ter acesso a dados pessoais na medida do que seja necessário para fornecer esses serviços.
5. O ISEC e a Aliança Portuguesa de Blockchain enquanto responsáveis pelo tratamento garantem o cumprimento rigoroso das normas de confidencialidade relativas aos dados disponibilizados.
6. O acima exposto não obsta a que o titular dos dados possa exercer os seus direitos de acesso, retificação, apagamento, limitação e oposição ao tratamento, enviando uma mensagem de correio eletrónico para info@all2bc.com, fazendo prova da sua identidade através do seu documento de identificação ou outro meio comprovativo adequado.

XI. Direitos de personalidade
1. Os participantes autorizam o ISEC e a Aliança Portuguesa de Blockchain a utilizar o seu nome e a sua imagem no âmbito da sua participação no Concurso, através de qualquer forma ou meio de reprodução, tanto eletrónico (Internet e outros análogos), como convencional (papel, fotografias e outros análogos), pela máxima duração permitida por lei.
2. Os participantes autorizam a entidade organizadora (Aliança Portuguesa de Blockchain) e parceiros a construir material audiovisual durante o desafio e a conferência sobre os participantes. Todo o material audiovisual (fotografia e vídeo) produzido é propriedade da entidade organizadora (APB).
3. O uso e publicação das imagens e dados do interessado na sua condição de vencedor conforme o exposto no presente Regulamento, não gera nem outorga reembolso, pagamento de compensação ou de direitos económicos de qualquer tipo para o vencedor.

XII. Propriedade Intelectual
A titularidade dos direitos de propriedade intelectual será, caso o desenvolvimento e as contribuições para a solução proposta o venham a justificar, definida através de acordo a celebrar com vista à repartição de titularidade e benefícios da sua exploração comercial.

ANEXO

Contexto

Informações sobre mais de 180.000 ataques terroristas
O Global Terrorism Database (Banco Mundial de Terrorismo - **GTD**) é uma base de dados de código aberto que inclui informações sobre ataques terroristas em todo o mundo de 1970 a 2017. O GTD inclui dados sistemáticos sobre incidentes terroristas internos e internacionais que ocorreram durante esse período e agora inclui mais de 180.000 ataques. A base de dados é mantida por investigadores do Consórcio Nacional para o Estudo do Terrorismo e Respostas ao Terrorismo (START), sediado na Universidade de Maryland. Mais Informação

Conteúdo

Geografia: Mundial
Período: 1970-2017, *exceto 1993*
Unidade de analise: Ataque
Variáveis: >100 variáveis sobre localização, táticas, perpetradores, alvos e resultados
Fontes: Peças jornalísticas não confidenciais (**Nota**: Por favor, interprete as alterações ao longo do tempo com cautela. Padrões globais são determinados por diversas tendências em certas regiões, e a recolha de dados é influenciada por flutuações no acesso à cobertura da mídia ao longo do tempo e o local).
Definition of terrorism:
"A ameaça ou o uso real de força e violência ilegal por uma entidade não-estatal para atingir um objetivo político, econômico, religioso ou social através de medo, coerção ou intimidação."
Ver GTD Codebook para detalhes sobre a metodologia de recolha de dados, definições e esquema de codificação.

Menções

A Base de Dados Global sobre Terrorismo é financiado pelo START, pelo Departamento de Estado dos EUA (Número do Contrato: SAQMMA12M1292) e pelo Programa Universitário da Direção de Ciência e Tecnologia do Departamento de Segurança Interna (Prêmio Número 2012-ST-061-CS0001, CSTAB 3.1) . As decisões e classificações de codificação contidas na base de dados são determinadas independentemente por investigadores do START e não devem ser interpretadas como representando necessariamente as visões ou políticas oficiais do governo dos Estados Unidos.
GTD Team

Publicações

O GTD tem sido alavancado em publicações académicas, relatórios, e peças jornalísticas. *Putting Terrorism in Context: Lessons from the Global Terrorism Database*, pelos investigadores principais do GTD LaFree, Dugan, e Miller que investigam padrões de terrorismo e apresentam perspetivas para os desafios da recolha de dados e análise. O gestor de dados da GTD, Michael Jensen, discute Benefits and Drawbacks of Methodological Advancements in Data Collection and Coding.

Fonte

Website: http://start.umd.edu/gtd

Termos de Uso

O uso dos dados significa sua concordância com os seguintes termos e condições.
CONTRATO DE LICENÇA DE UTILIZADOR FINAL COM A UNIVERSIDADE DE MARYLANDIMPORTANT – ESTE É UM ACORDO LEGAL ENTRE VOCÊ ("Você") E A UNIVERSIDADE DE MARYLAND, uma agência pública e instrumental do Estado de Maryland, pelo e através do Consórcio Nacional para o Estudo do Terrorismo e Respostas ao Terrorismo ("START", " EUA", " WE "ou" Universidade "). POR FAVOR, LEIA ESTE ACORDO FINAL DE LICENÇA DE UTILIZADOR ("EULA") ANTES DE ACEDER A Base de Dados Globais sobre Terrorismo ("GTD"). OS TERMOS DESTE EULA REGULAM O SEU ACESSO E UTILIZAÇÃO DO WEBSITE GTD, DOS DADOS, DO CÓDIGO E DE QUALQUER MATERIAL AUXILIAR. AO ACEDER AO GTD, SIGNIFICA QUE LEU, COMPREENDE, ACEITA E CONCORDA EM ACEITAR ESTES TERMOS E CONDIÇÕES. SE VOCÊ NÃO ACEITAR OS TERMOS DESTE EULA, NÃO ACEDA O GTD.

TERMOS E CONDIÇÕES

1. **GTD significa Base de Dados sobre Terrorismo Global** e a interface de utilizador on-line **(www.start.umd.edu/gtd)** produzidas e mantidas pelo Consórcio Nacional para o Estudo do Terrorismo e Respostas ao Terrorismo (START). Isso inclui os dados e o livro de códigos, quaisquer materiais auxiliares presentes e a interface do usuário pela qual os dados são apresentados.

2. **CONCESSÃO DE LICENÇA**. A Universidade concede a você um direito revogável, não exclusivo e intransferível para aceder o GTD e usar os dados, o livro de códigos e quaisquer materiais auxiliares exclusivamente para pesquisa e análise não comerciais.

3. **RESTRIÇÕES** Você concorda em NÃO: a) publicamente publicar ou exibir os dados, o livro de códigos, ou quaisquer materiais auxiliares sem permissão expressa por escrito pela Universidade de Maryland (isso exclui publicação de análise ou visualização dos dados para fins não comerciais); b) vender, licenciar, sub licenciar ou distribuir os dados, o livro de códigos ou quaisquer materiais auxiliares a terceiros por dinheiro ou outras considerações; c) modificar, ocultar, excluir ou interferir com quaisquer avisos incluídos no GTD ou no livro de códigos, ou quaisquer materiais auxiliares; d) usar o GTD para tirar conclusões sobre o status legal oficial ou antecedentes criminais de um indivíduo, ou o status de uma investigação criminal ou civil; e) interferir ou interromper o site ou servidores e redes da GTD conectados ao site da GTD; ou f) use robôs, spiders, crawlers, dispositivos automatizados e tecnologias semelhantes para recolher dados do site ou se envolver na agregação de dados ou na indexação dos dados, do livro de códigos ou de qualquer material auxiliar que não esteja de acordo com o arquivo robots.txt do site.

4. **AS SUAS RESPONSABILIDADES:** a) Todas as informações provenientes do GTD devem ser reconhecidas e citadas da seguinte forma: "Consórcio Nacional para o Estudo do Terrorismo e Respostas ao Terrorismo (START), Universidade de Maryland. (2018). Base de Dados Globais sobre Terrorismo (GTD)." Obtido de https://www.start.umd.edu/gtd" b) Você concorda em reconhecer qualquer material com direitos autorais com um aviso de direitos autorais "Copyright University of Maryland 2018". c). Quaisquer modificações feitas ao GTD para análise publicada devem ser claramente documentadas e não devem deturpar as decisões analíticas tomadas pelo START. d) Você concorda em procurar um contrato adicional para usar o GTD, os dados, o livro de códigos ou materiais auxiliares para fins comerciais, ou para criar produtos comerciais ou serviços baseados no GTD, nos dados, no livro de códigos ou nos materiais auxiliares.

5. **PROPRIEDADE INTELECTUAL.** A Universidade possui todos os direitos, título e interesse no GTD, nos dados e no livro de códigos e em todos os materiais auxiliares. Este EULA não concede a Você nenhum direito, título ou participação no GTD ou nos dados, no livro de códigos, na interface do utilizador ou em quaisquer materiais auxiliares que não sejam aqueles expressamente concedidos a você sob este EULA.

6. **ISENÇÃO E LIMITAÇÃO DE RESPONSABILIDADE**. a). O GTD, o CODEBOOK, a INTERFACE DO UTILIZADOR OU TODOS OS MATERIAIS AUXILIARES SÃO DISPONIBILIZADOS "COMO ESTÃO". A UNIVERSIDADE REJEITA TODAS E TODAS AS DECLARAÇÕES E GARANTIAS - SEJAM EXPRESSAS OU IMPLÍCITAS, ORAL OU ESCRITA, DE FATO OU DECORRENTE DA LEI - EM RELAÇÃO À GTD, AO CÓDIGO E A QUALQUER MATERIAL AUXILIAR, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS DE COMERCIAL, QUALIDADE SATISFATÓRIA, ADEQUAÇÃO A UM FIM ESPECÍFICO E NÃO VIOLAÇÃO DA PROPRIEDADE INTELECTUAL OU DIREITOS DE PROPRIEDADE DE TERCEIROS. A UNIVERSIDADE NÃO FAZ NENHUMA REPRESENTAÇÃO OU GARANTIA DE QUE A GTD, O CODEBOOK, QUAISQUER MATERIAIS AUXILIARES OU A INTERFACE DO UTILIZADOR FUNCIONARÃO LIVRE DE ERROS OU DE FORMA ININTERRUPTA. b) Em nenhuma circunstância a Universidade será responsabilizada por quaisquer danos incidentais, especiais, punitivos, exemplares ou consequenciais de qualquer tipo, incluindo perda de lucros ou interrupção de negócios, mesmo se avisada da possibilidade de tais reivindicações ou exigências, seja em contrato, ato ilícito ou de outra forma, surgindo em conexão com o Seu acesso e uso do GTD, o livro de códigos, a interface do usuário ou quaisquer materiais auxiliares ou outras transações. Essa limitação sobre danos e reivindicações deve ser aplicada sem considerar se outras disposições deste EULA foram violadas ou se mostraram ineficazes. Em nenhuma circunstância a responsabilidade total da Universidade pela violação ou não cumprimento deste EULA excederá

as taxas pagas à Universidade dentro do atual ciclo de financiamento. c) Todo esforço razoável foi feito para verificar as fontes e verificar fatos no GTD; no entanto, o START não pode garantir que as contas relatadas na literatura aberta sejam/estejam completas e precisas. A START não se responsabiliza por qualquer perda ou dano causado por erros ou omissões ou resultante de qualquer uso, uso indevido ou alteração dos dados da GTD pelo UTILIZADOR. O UTILIZADOR não deve deduzir quaisquer ações ou resultados adicionais além do que é apresentado em uma entrada GTD e, especificamente, o UTILIZADOR não deve inferir que um indivíduo referenciado no GTD foi acusado, julgado ou condenado por terrorismo ou qualquer outro crime. Se uma nova documentação sobre um evento se tornar disponível, o START pode modificar os dados conforme necessário e apropriado. d) A Universidade não tem obrigação de atualizar o GTD, o livro de códigos, a interface do usuário ou qualquer material auxiliar.

7. I**NDEMNIZAÇÃO** Você concorda em defender, indemnizar e inocentar a Universidade e os seus funcionários, agentes, diretores e executivos de e contra todas e quaisquer reclamações, processos, danos, lesões, responsabilidades, perdas, custos e despesas (incluindo advogados razoáveis). taxas e despesas de litígio) relacionadas com, ou decorrentes do uso do GTD, do livro de códigos, ou de quaisquer materiais auxiliares ou Sua violação de qualquer termo neste EULA.

8. **PRAZO E TERMO** a) Este EULA e seu direito de aceder ao site da GTD e usar os dados, o livro de códigos e quaisquer materiais auxiliares entrarão em vigor quando você aceder o GTD. b) A Universidade reserva-se o direito de, a qualquer momento e sem aviso prévio, modificar, descontinuar ou suspender, temporária ou permanentemente, o seu acesso ao site da GTD (ou qualquer parte dele) sem responsabilidade perante você.

9. **DIVERSOS** a) A Universidade pode modificar este EULA a qualquer momento. Verifique o site da GTD para obter modificações. b) Nenhum termo deste Contrato pode ser renunciado exceto pelo consentimento por escrito da parte renunciando ao cumprimento. c) Se qualquer disposição deste EULA for determinada por um tribunal de jurisdição competente como nula, inválida ou de outra forma inexequível, tal determinação não afetará as demais disposições deste Contrato. d) Este Contrato não cria uma relação de joint venture, parceria, emprego ou agência entre as Partes. e) Não há terceiros beneficiários deste acordo. Você não pode atribuir este contrato sem a aprovação prévia por escrito da Universidade. f) Este EULA será regido e interpretado de acordo com a lei de direitos autorais dos Estados Unidos e as leis do Estado de Maryland, sem referência às regras de conflito de leis. Nada neste EULA é ou deve ser considerado como uma renúncia pela Universidade de qualquer um dos seus direitos ou status como uma agência e instrumento do Estado de Maryland. As partes concordam mutuamente em recusar a aplicação do (MUCITA) (Maryland Uniform Computer Information Transactions Act), o Código de Maryland Anotado [Lei Comercial] 21-101 até 21-816, na medida máxima autorizada pela MUCITA. g) Este EULA representa o acordo completo entre Você e a Universidade com relação ao assunto dos parágrafos 1-10. Não existem outros entendimentos, escritos ou orais, que não estejam incluídos neste Contrato.

10. **REPRESENTAÇÃO** Você declara que tem pelo menos 18 anos de idade.

TREINO

A START lançou o primeiro de uma série de módulos de formação projetados para equipar os utilizadores da GTD com o conhecimento e as ferramentas para melhor aproveitar a base de dados. Este módulo de formação fornece uma visão geral do GTD, incluindo o processo de recolha de dados, usos do GTD e padrões de terrorismo global. Os participantes aprenderão como lidar com dados básicos e como gerar estatísticas de resumo do GTD usando Tabelas Dinâmicas no Microsoft Excel.