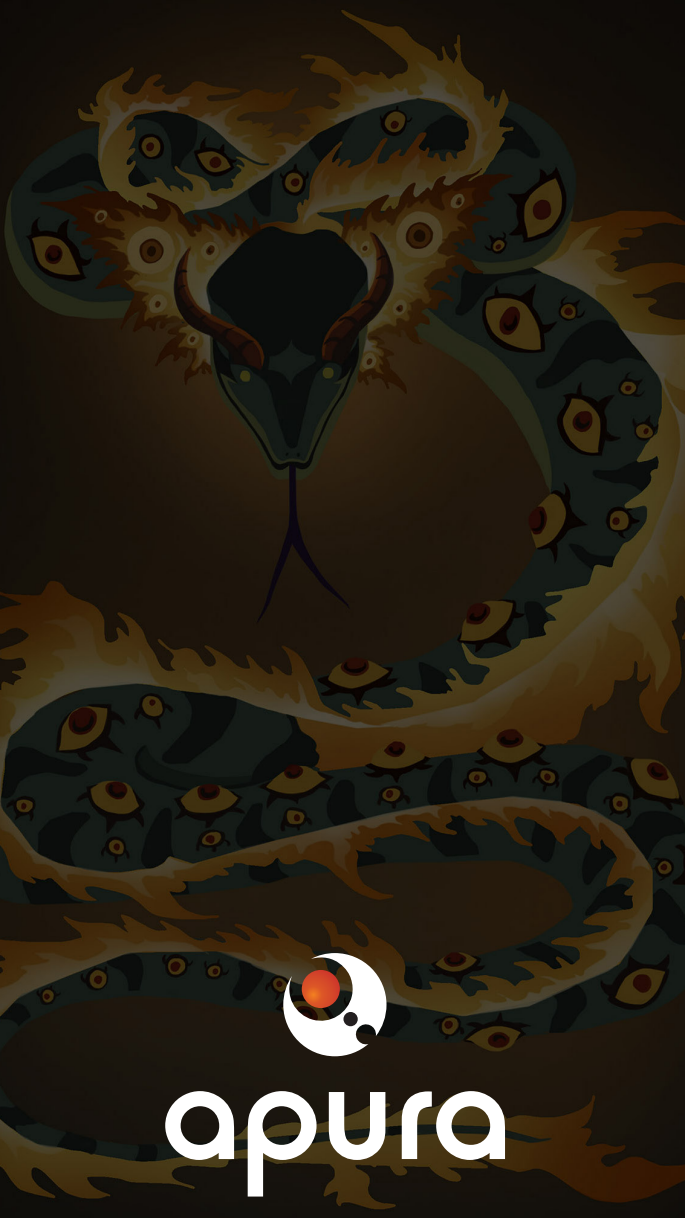
Inteligência em fontes abertas

BTT NG



apura

A quantas ameaças sua organização está exposta?

UMA DICA: MAIS DO QUE VOCÊ ESTÁ PREPARADO PARA LIDAR. ENTÃO, PREPARE-SE!

Em um mundo onde novas e cada vez mais sérias ameaças surgem a todo instante, o cenário ideal é estar sempre à frente dos adversários, recebendo informações de fontes fidedignas, confiáveis, atualizadas e disponíveis.

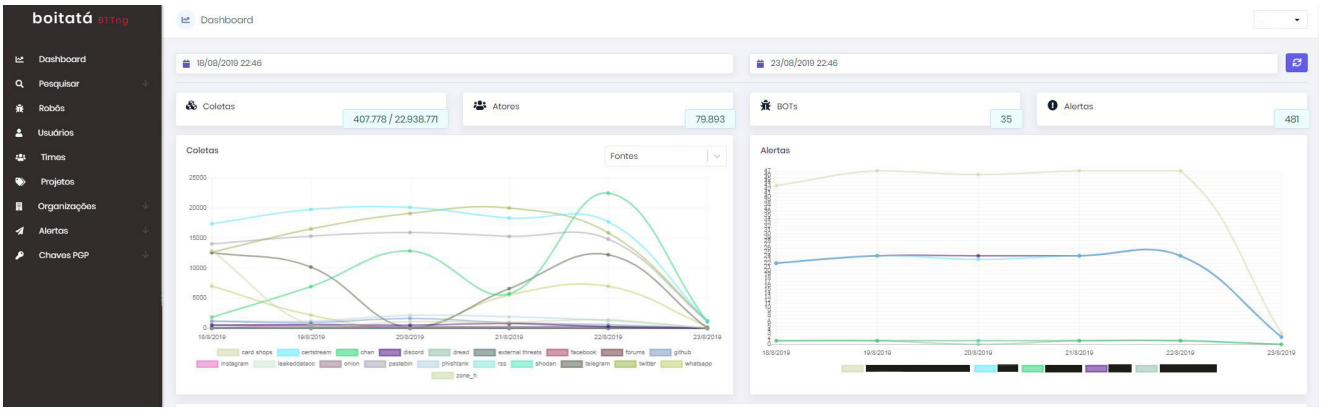
O **BTT** NG (também conhecido como Boitatá Next Generation), plataforma proprietária de Open Source Intelligence criada e mantida pela Apura Cybersecurity Intelligence, automatiza as fases de coleta, busca e indexação de informações existentes na Web (Clear Web), em redes sociais, além da Dark/Deep Web.

COMO FUNCIONA

O **BTT** NG permite obter informações sobre as mais diversas ameaças, cibernéticas, negociais, situacionais, sejam elas internas ou externas. Por meio de dezenas de robôs, a ferramenta coleta milhares de informações todos os dias, em diversas fontes, acrescentando dados a uma base que já contém dezenas de milhões de entradas.

Os robôs podem ser customizados para atingir os objetivos específicos da organização e novos robôs são desenvolvidos constantemente para dar uma visibilidade ainda mais profunda e ampla do ambiente de ameaças.

A ferramenta oferece uma grande flexibilidade na pesquisa das informações indexadas, dando agilidade e reduzindo a ocorrência de falso-positivos, garantindo visibilidade fidedigna do bioma cibercriminoso e dos riscos cibernéticos a que a organização está exposta.



RECURSOS

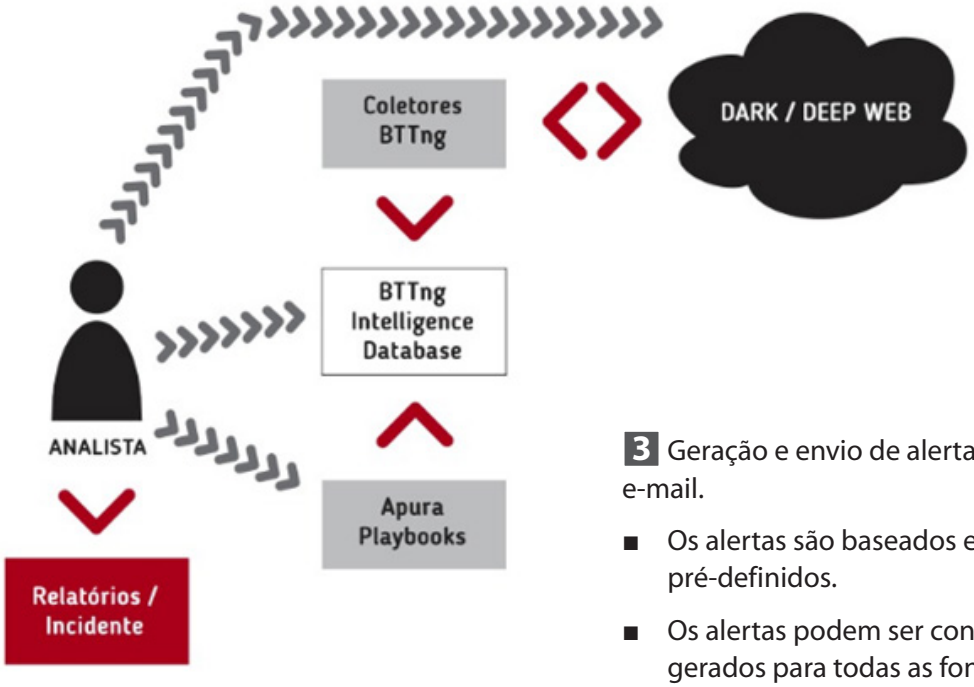
1 A ferramenta tem a capacidade de pesquisar e alertar quando atividades mal-intencionadas forem detectadas. Possíveis fraudes, ameaças internas, ameaças cibernéticas, ocorrências decorrentes de respostas a incidentes de segurança da informação, ameaças à imagem da organização, mal uso de redes sociais, risco de perda de dados, sejam quais forem as ameaças, o **BTT** NG está preparado para detectar, avaliar, filtrar e alertar a organização o quanto antes:

- Tenha visibilidade de novas vulnerabilidades descobertas nos sistemas operacionais mais utilizados: Windows (10 e anteriores), Linux (Ubuntu, CentOS, RedHat, entre outras), MacOS, OpenBSD, Android, iOS, etc.
- Saiba quando ataques utilizando tais vulnerabilidades forem bem sucedidos; entenda o modus operandi dos atacantes por meio de casos reais.
- Monitore seus serviços on-line e internos que estejam expostos de forma inapropriada, sem a devida restrição de acesso.
- Obtenha informações sobre novos malwares e campanhas a eles associadas.
- Tem capacidade de reconhecer endereços de e-mail que constem em listas de SPAM, coletadas automaticamente, e gerar alertas padronizados ou customizados.

- Seja informado quanto à alteração de informações de registro de um domínio ou, ainda, quando novos domínios potencialmente maliciosos forem criados (inclusive sites registrados com nomes semelhantes, aproximados, permutados, typosquatting).
- Receba alertas referentes a vazamento de dados, em especial dados confidenciais, credenciais e outras informações que colocam uma organização em risco.
- Descubra se credenciais da sua organização estão sendo comercializadas em mercados ilegais on-line ou físicos.
- O **BTT** NG detecta páginas de phishing, identificando informações de registro em entidades reguladoras, correlacionando com outros ataques semelhantes. Em última instância, é possível remover o conteúdo malicioso[1].
- Identifica aplicativos falsos e maliciosos em lojas de aplicativos. Em última instância, é possível remover o conteúdo malicioso[1].

2 Permite a criação de relatórios e gráficos customizados, além de dashboards.

- É possível exportar os resultados em diferentes formatos, como .csv, .pdf, .html, .docx, .txt, além de programar o envio por e-mail.
- Os relatórios podem ser gerados na periodicidade que o cliente precisar, por dia, semana, mês ou ano.



3 Geração e envio de alertas em tempo real via e-mail.

- Os alertas são baseados em palavras ou termos pré-definidos.
- Os alertas podem ser configurados para serem gerados para todas as fontes ou algumas específicas.
- Podem ser enviados em diferentes formatos, para facilitar a triagem e tomada de decisão. É possível enviar e-mail para uma ou mais pessoas através de listas de distribuições.

1. Serviço licenciado separadamente.

4 Pesquisas com base em palavras-chave, utilizando sintaxe Lucene ou Regex.

5 Obtenha informações atualizadas sobre campanhas hacktivistas passadas, em andamento ou em fase de planejamento.

- Monitoramento de fóruns específicos de hacktivismo, bem como perfis em redes sociais de grupos e indivíduos ligados à atividade.
- A ferramenta está apta a detectar campanhas de defacement, de ataques DDoS, de extorsão, de divulgação de malwares, entre outras ações de atores maliciosos.

6 Proteja sua propriedade e sua marca.

- Identifique campanhas fraudulentas associadas aos seus produtos/serviços sendo divulgadas na Web, Deep/Dark Web ou em redes sociais.
- Conheça vulnerabilidades ou bugs em seus produtos/serviços que permitem que terceiros mal-intencionados tirem proveito e causem prejuízo.
- Saiba quando estiverem comercializando algum produto ou serviço de sua propriedade de forma inadequada ou ilegal ou para fins diferentes dos quais foram elaborados.
- Detecte sites/domínios falsos relacionados a seus produtos. Identifique também perfis falsos em redes sociais. Em última instância, é possível remover o conteúdo malicioso.

SOBRE A FERRAMENTA

- Licenciamento por número de usuários com acesso a plataforma, não havendo limitação de quantidade usuários simultâneos.
  - É possível criar diferentes perfis de acesso, customizando as permissões individuais.
  - O usuário pode possuir acesso ilimitado a todas as funcionalidades da ferramenta, com login e senha próprios que ele poderá gerenciar.
  - Crie organizações, times e projetos para ter melhor controle do acesso e atribuição de responsabilidades no uso da ferramenta.
- Possui versões on-premise ou em nuvem.
- Permite a encriptação dos alertas com chave PGP.
- A ferramenta possui integração via API Rest .

facebook.com/apura.oficial
twitter.com/apura_oficial

http://apura.com.br

São Paulo - (11) 5504-1966
Brasília - (61) 3255-1245

apura

Inteligência em fontes abertas

BTT NG