

# MANTIS

## IDENTIFIQUE AMEAÇAS ANTES DO IMPACTO

### FICHA TÉCNICA

#### Conheça a ferramenta número um para identificação de ameaças.

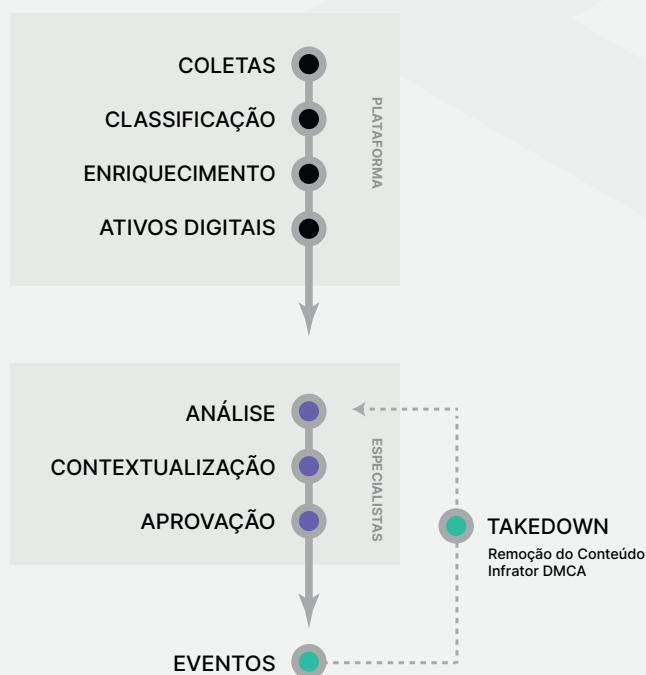
O Mantis é uma solução de proteção e monitoramento de riscos digitais, também conhecida como DRPS - Digital Risk Protection Services. É uma combinação de plataformas tecnológicas, processos de inteligência de dados e profissionais especializados em Pentests, OSINT e Threat Hunting.

A Plataforma busca por riscos digitais em milhares de pontos na Internet, acelerando a amplitude de visibilidade e a profundidade da proteção dos ativos digitais em uma organização, melhorando significativamente a capacidade de se antecipar e mitigar prejuízos e impactos financeiros e de reputação de marca.

“Os serviços de proteção de riscos digitais melhoram a capacidade de uma organização de detectar, priorizar e responder a ameaças on-line em qualquer lugar onde os ativos digitais estão expostos e em risco.”

RELATÓRIO DO GARTNER DE 2020 TECNOLOGIAS EMERGENTES: INSIGHTS CRÍTICOS EM SERVIÇOS DE PROTEÇÃO DE RISCO DIGITAL

### FLUXO DO SISTEMA



#### Remova riscos digitais, mitigue o impacto.

##### Proteção de Marca

A transformação digital e a mudança para o home office deixaram ferramentas de segurança tradicionais sem visibilidade de novas ameaças.

##### Segurança Proativa

Proteja os ativos digitais críticos por meio de inteligência de ameaças, com intervenção contra personificação de marca, vazamento de dados, ameaças de mídia social, aquisição de contas e outros riscos digitais.

##### Cenário Brasileiro

O Mantis tem como foco as fraudes digitais ocorridas no mercado brasileiro, envolvendo empresas nacionais, diferente de soluções do mercado cujo foco não é o Brasil.

#### Tenha total visibilidade de superfície de ataques e reduza riscos.

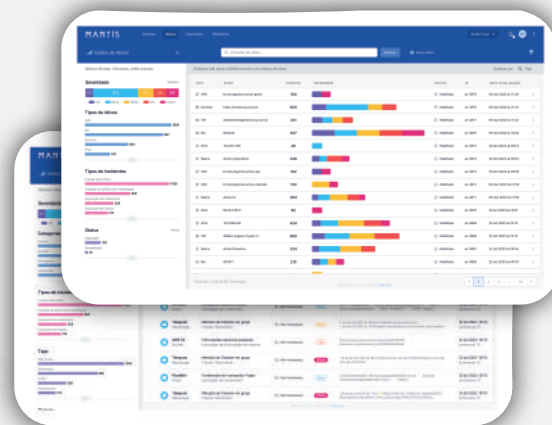


## Processamento de Linguagem Natural (NLP)

Tecnologia capaz de descobrir o que uma menção ou um evento detectado significam, seja em forma visual ou de áudio. Ao lidar com as nuances da linguagem humana ou natural, como erros ortográficos, gírias ou termos informais, permite a compreensão de contextos de engenharia social, a tradução automática em diversas línguas e também sentimentos negativos em mensagens. Com isso, ajuda a contextualizar intenções maliciosas por trás de uma ação de um cibercriminoso.

## Leitura de Imagens e Transcrição de Áudios

Se conversas de ataque detectadas em canais de mensagens privadas e fóruns da dark web não ocorreram por meio de texto, mas através de imagens e troca de áudios, o Mantis varre e transcreve o conteúdo, em um monitoramento profundo dos ativos da marca. Isso também é feito em relação a registros de domínio, contas de mídia social e e-mail para nomes/imagens da empresa e de produtos, em situações de reclamação fraudulenta, anúncios e ataques de coleta de credenciais.



## Monitoramento de certificados SSL emitidos

Monitora os domínios assinados pelas principais autoridades certificadoras, permitindo que a empresa identifique possíveis sites maliciosos utilizando os nomes ou domínios similares ao seu negócio. É um motor em potencial para identificação de phishing com certificados SSL recém-emitidos.

## Análise automática de aplicativos móveis

O Mantis pode identificar fragilidades expostas dentro de aplicativos móveis dentro da Google Play, como chaves, API URLs, senhas e pontos de informações sensíveis.

## Detecções através de tecnologia proprietária Mantis Tracking

É bastante comum que sites maliciosos de Phishing redirecionem a vítima para o site oficial após a coleta de dados ou credencial. Agora, imagine um cenário onde um agente malicioso está desenvolvendo ou testando uma página falsa e maliciosa do site oficial da empresa. Através do Mantis Tracking conseguimos detectar e analisar este tipo de site malicioso antes mesmo do agente suspeito iniciar uma campanha. Com um simples passo de habilitação em seu site nossos coletores conseguem analisar e revisar se os acessos com origens suspeitas apresentam algum tipo de risco digital.

## Gestão de Alertas

Gestão de alertas que podem ser configurados com super granularidade, indicando quem recebe qual alerta com base no tipo, severidade, Keywords, etc.

Configuração de Alertas de forma personalizada através dos campos: Tipo de Incidente, Origem, Severidade, Palavra-Chave e Operador.

Alertas gerados com descrição de cada caso, impacto esperado, recomendações de mitigação.

## Acompanhamento Personalizado

Reuniões de acompanhamento mensais com cada cliente para feedback e detalhamento dos riscos identificados.

## Integração

Integração via API Rest para flexibilidade no modo de uso do serviço pelo cliente.


Integração com SIEMs através do envio dos alertas no formato CEF.


### Serviço Mantis


- Licenciamento limitado de Ativo Digital por empresa
- Pacote de Takedowns Mensais
- Pesquisa e Investigação Aprofundada
- Equipe de Threat Intel Avançado
- Relatórios Ilimitados
- Score de Risco por Ativo Digital


### Entre em Contato

Invista na segurança digital de sua empresa!

 (11) 97492.6049

 contato@safelabs.com.br

 R. Leocádia Pedra dos Santos, 115, Ed. Base 27, sala 212 - Enseada do Suá, Vitória - ES, 29050-370

 SafeLabs.com.br

# MANTIS