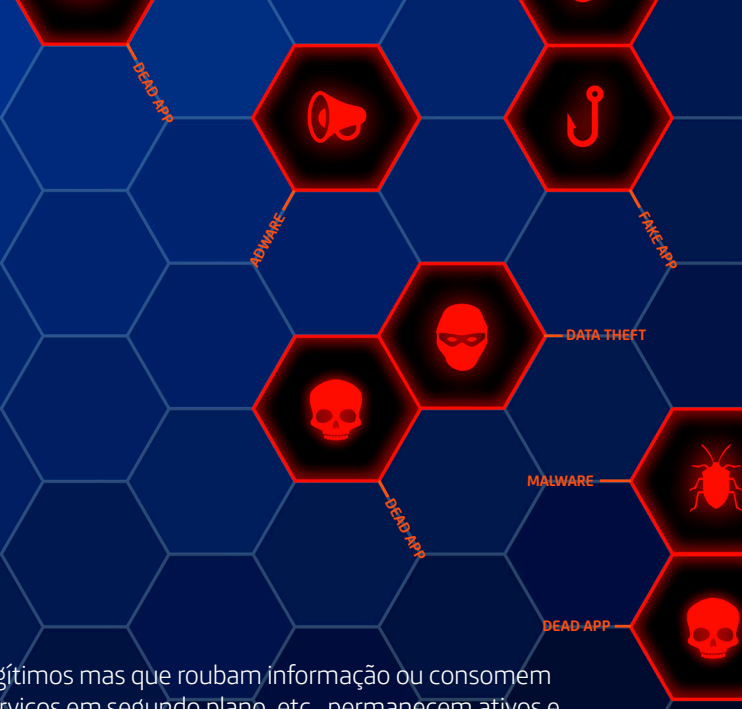
Tacyt

The tool for
app cyber intelligence



Monitorização e análise de ameaças móveis

Tacyt é uma inovadora ferramenta de ciberinteligência que facilita aos profissionais e especialistas em segurança a pesquisa em ambientes de aplicativos móveis através de sua tecnologia de big data.

As ameaças contra a segurança relacionadas com o mundo móvel crescem continuamente: ataques específicos, adware agressivo, imitações de aplicativos que se comportam como legítimos mas que roubam informação ou consomem serviços em segundo plano, etc., permanecem ativos e disponíveis nos Market Places o tempo suficiente para afetar milhares de usuários.

Tacyt permite a rápida detecção, descoberta e análise destas ameaças para reduzir o seu impacto potencial nas organizações.

Tacyt supervisiona, armazena, analisa, correlaciona e classifica milhões de apps móveis, adicionando milhares de aplicativos novos a cada dia

Inovação
Nova ferramenta a serviço de analistas e especialistas em segurança

Inteligência
Tecnologia patenteada para a correlação e inteligência aplicável

Frescor
Análise dinâmica do App Market por intermédio de consultas simples

Visão global
Avaliação do aplicativo e de suas circunstâncias: quando, quem, o que, onde

Versatilidade
Ferramenta versátil e de alto rendimento acessível para empresas e especialistas

Benefícios

- Acesso a toda a informação associada a um aplicativo: metadados, licenças, desenvolvedor, arquivos, urls que acesse, etc.
- Consulta, comparação e vinculação de aplicativos que compartilham qualquer dado indexado na plataforma.
- Detecção e prevenção de fraude contra clientes ou funcionários (malware, adware, roubo de credenciais, descumprimento de políticas, etc.).
- Detecção de ameaças contra a marca de uma empresa.
- Identificação de padrões suspeitos como: desenvolvedores com histórico de fraude, aplicativos que compartilham certificados, etc.
- Identificação do modus operandi para determinar quem está por trás, outras campanhas e aplicativos associados, conhecer o seu histórico completo, e antecipar os seguintes ataques.

A quem se destina?

Tacyt foi pensado para empresas que:

- Queiram reduzir seu risco contra ameaças associadas aos apps.
- Desejem monitorizar de forma proativa o aparecimento de apps "imitadores".
- Fabricantes e fornecedores de serviços de segurança ou ciberinteligência.
- Pesquisadores e analistas de segurança.
- Fornecedores de serviços de segurança gerenciada (MSSP).
- Órgãos responsáveis pela aplicação da lei (LEA, FCS, etc.).

Tacyt

Um ecossistema de ciberinteligência móvel

Tacyt oferece um completo conjunto de funções que melhoram a análise e a pesquisa para dar resposta a qualquer ação fraudulenta na qual algum componente móvel possa ter sido utilizado. Tacyt permite que os analistas façam um seguimento da atividade destes desenvolvedores de componentes móveis e prevejam outras possíveis ações que tenham realizado.

Tacyt também permite estabelecer alertas que detectem a atividade realizada por desenvolvedores maliciosos, transformando-se assim em uma solução completa para as equipes de segurança, legais ou de marketing, ou para analistas de tendências de apps móveis.

Características técnicas

Potente motor de busca que permite analisar e filtrar com base em diferentes parâmetros: datas, tamanho, imagens, relações entre APKs, dados circunstanciais, desenvolvedores, criptografia, software, etc.

Filtros fáceis de criar, com alertas em tempo real e possibilidade de compartilhamento. Apoia-se em diferentes metodologias de correlação que permitem classificar a informação e facilitam a pesquisa e a análise.

Atualização imediata dos aplicativos e suas circunstâncias quando se modificam nos markets. Possibilidade de assinatura a filtros oficiais, públicos e avançados que são melhorados continuamente.

Seu API permite interagir com a informação de forma programada e a comunicação com outro software. A análise de APKs externos pode ser automatizada para se integrar com qualquer outra ferramenta.

O Tacyt pode ser adquirido como um produto independente ou como um serviço gerenciado e operado pela Telefónica

		Organizações	PVA*
CASOS DE USO	Detecção de ameaças contra a marca de uma empresa.	SIM	SIM
	Reconhecimento de versões maliciosas de apps oficiais	SIM	SIM
	Identificação de apps, padrões e atacantes suspeitos	SIM	SIM
	Pesquisa de casos de apps móveis falsos	SIM	SIM
	Criação de perfis de atacantes, suas técnicas, táticas e procedimentos (TTPs)	SIM	SIM
INTEGRACOM	Soluções antivírus aumentando a detecção de apps móveis maliciosos	NÃO	SIM
	Soluções tecnológicas de sandboxing e análise forense móvel	NÃO	SIM
	Tecnologias MDM	NÃO	SIM
	Outras integrações	NÃO	SIM

* Partners de Valor Agregado