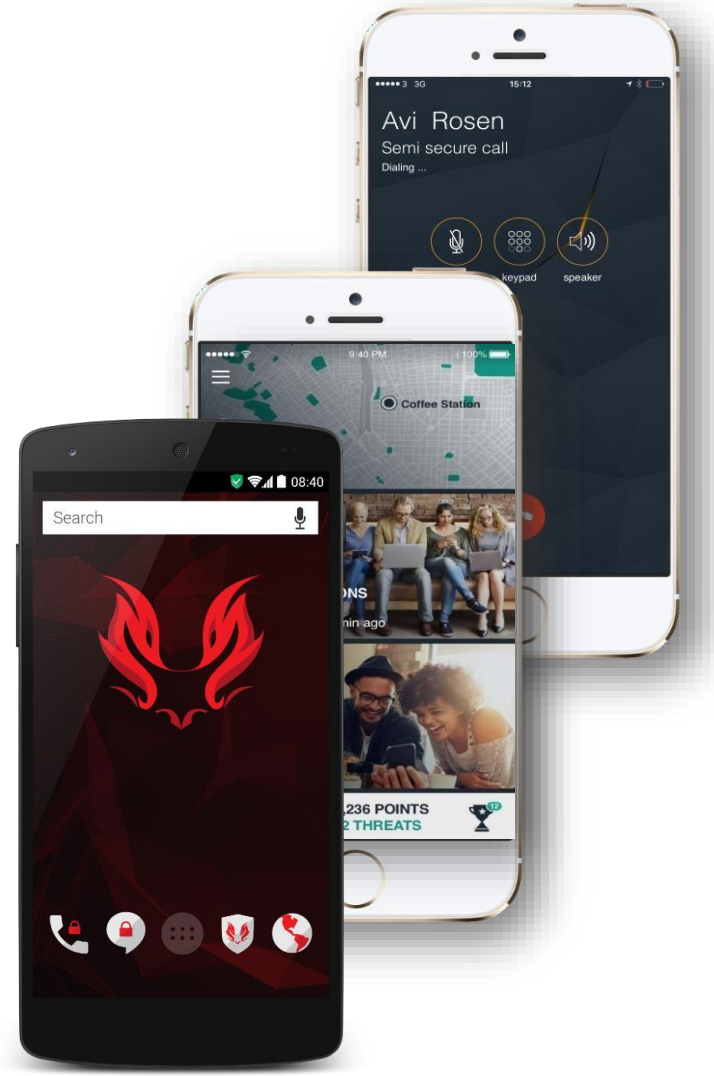

KAYMERA
Mobile security redefined
Citadel - Brasil
CITADEL
Oferece a mais recente tecnologia de segurança para smartphones

KAYMERA
Mobile security redefined

Citadel - Brasil

Quem é Kaymera?

- Fundada em 2013 por veteranos israelenses do setor de segurança cibernética, com experiência em métodos de coleta de inteligência móvel e ataque cibernético.
- A Kaymera oferece o sistema de defesa contra ameaças cibernéticas móvel mais avançado do mundo, projetado para proteger contra ameaças avançadas de segurança móvel.
- Segurança móvel de nível militar e uma experiência de usuário fácil do smartphone perfeitamente balanceado.
- Totalmente operacional em várias entidades e organizações governamentais em todo o mundo.



KAYMERA
Mobile security redefined

Citadel - Brasil

A nova era das ameaças móveis

O aumento da mobilidade no mundo moderno causou uma drástica mudança na forma de empresas e pessoas se comunicarem ou trabalharem. Esta mudança que afeta o trabalhador e o fato de as pessoas estarem sempre conectadas, em casa e fora dela, aumenta o nível de exposição de dados corporativos confidenciais. Altos funcionários usam seus celulares extensivamente e normalmente não têm consciência das ameaças envolvidas. Até poucos anos atrás os empregados estavam acostumados a trabalhar em um ambiente onde tudo era controlado, seguindo as estritas orientações de segurança de TI (laptops e desktops). Hoje, com o onipresente BYOD, os usuários estão habituados a combinar uso pessoal e profissional em seus celulares e fazem download e instalação de aplicativos sem considerar o potencial risco de interceptação das comunicações ou de infecção por vírus. A implicação direta é a potencial exposição dos dados confidenciais de negócios. Imagine uma conversa de um executivo de alto nível sendo interceptada por um dispositivo tático (IMSI catcher/Rogue BTS) enquanto discute o último desempenho financeiro da empresa ou um telefone infectado por um vírus ou por um aplicativo nocivo que use o microfone do celular para espionagem e sejam levados para uma sala onde a estratégia da empresa ou a inovação de produtos estejam sendo discutidas. Com o incrível crescimento de aparelhos celulares no mundo, o número de vírus em aparelhos cresceu em quantidade e sofisticação, se tornou um sério problema e um risco real para a segurança.

Pesquisas mostram que nove entre 10 americanos usam seus celulares para trabalhar e 50% se conectam a redes sem fio inseguras. Mais de 50% dos dispositivos não têm sequer uma senha de proteção. Todo celular está em perigo – até o celular de Angela Merkel já foi grampeado. O FBI utiliza seu sistema Stingray de detectores de IMSI para acessar uma torre de celular legítima e interceptar celulares ou qualquer outro dispositivo móvel. Pacotes de vírus altamente sofisticados, sistemas de ataque WiFi MitM ou detectores de IMSI estão se tornando cada vez mais disponíveis no mercado. Por apenas alguns mil dólares é possível comprar um equipamento legítimo de rede, usar um laptop com apenas alguns aplicativos e será possível construir um poderoso caçador de IMSI que pode interceptar qualquer chamada telefônica em um raio de 300 metros.

Como dispositivos móveis se tornaram uma das mais perfeitas ferramentas de coleta de informações, as ameaças são mais complexas e mais difíceis de serem detectadas e protegidas.

KAYMERA
Mobile security redefined

Citadel - Brasil

As ameaças a dispositivos móveis estão aumentando

Proteger as informações contra violações é um desafio crítico para todas as organizações, e mais difícil ainda devido ao aumento do acesso a essas informações por parte dos dispositivos móveis utilizados pelos funcionários. Os gerentes de segurança se esforçam para equilibrar a segurança intransigente com a mobilidade dos funcionários e, portanto, devem implantar uma solução de segurança que proporcione funcionalidade abrangente com a escalabilidade e flexibilidade adequadas, promovendo o mais alto nível de segurança possível. As medidas de segurança são determinadas pelo nível de confidencialidade dos dados e o nível de risco dos mesmos.

MOBILIDADE é imprescindível para o aumento da produtividade e redução dos custos;
BYOD é cada vez mais uma realidade em todas as instituições e um pilar fundamental para a mobilidade.

… mas o RISCO é alto!


Aplicações maliciosas


Trojans


Interceptação de comunicação


Extração de dados físicos

KAYMERA
Mobile security redefined

WhatsApp é vítima de um dos ciberataques mais espetaculares dos últimos anos

rfi
14/05/2019 11h12

Um grupo de hackers explorou uma falha de segurança no WhatsApp e instalou um programa espião em celulares de usuários, confirmou a empresa nesta terça-feira (14). Este é um dos ciberataques mais espetaculares dos últimos anos e a atualização do aplicativo é altamente recomendada.

Um grupo de hackers explorou uma falha de segurança no WhatsApp e instalou um programa espião em celulares de usuários, confirmou a empresa nesta terça-feira (14). Este é um dos ciberataques mais espetaculares dos últimos anos e a atualização do aplicativo é altamente recomendada.

A vulnerabilidade de um dos aplicativos de mensagens instantâneas mais

Citadel - Brasil

javascript:window.open(window.clickTag)

globo.com g1 globoesporte gshow videos tecnologia
ASSINE JÁ MINHA CONTA E-MAIL ENTRAR
MENU techtudo DOWNLOADS BUSCAR

Ataque hacker no país preocupa brasileiros; saiba como se proteger

Média mundial do Índice de Segurança da Unisys é de 175 pontos, mas Brasil registra 190

Por Louise Rodrigues, da Redação
26/06/2019 07h00 · Atualizado há 3 semanas

O quanto você se preocupa com a segurança dos seus dados na internet? A resposta para essa pergunta é o pontapé para o **Índice de Segurança da Unisys**. O conhecido indicador anual mede como os usuários se sentem em relação à tecnologia e segurança digital. Em 2019 a conclusão é, também, um alerta: o índice é o maior dos últimos dez anos.

LEIA: **Carregadores públicos podem roubar seus dados; entenda**

HOME › NOTÍCIAS › Ataque cibernético em operadoras de telefonia rouba informações durante sete anos

Ataque cibernético em operadoras de telefonia rouba informações durante sete anos

27/06/2019 mindsecblog Notícias 1

Ataque cibernético em operadoras de telefonia rouba informações durante sete anos. Um ataque cibernético , provavelmente conduzido por hackers ligados ao governo chinês, atingiu ao menos dez operadoras de telefonia em diversos países, afirma a empresa de segurança Cybereason. Um relatório divulgado nesta terça-feira, dia 25 de junho, revela que os atacantes se infiltraram e se mantiveram ativos, roubando informações de alvos específicos, ao longo de ao menos sete anos. E pelo nível de controle alcançado, alerta a Cybereason, os hackers poderiam até mesmo desativar as redes de telefonia celular.

SEARCH ...

SIGA-NOS FACEBOOK

RECEBA NOSSA NEWSLETTER

Nome *
First Last

Empresa *
Nome da Empresa onde Trabalha

Cargo *

KAYMERA
Mobile security redefined

Citadel - Brasil

Smartphones - as melhores ferramentas para coleta de informações

Enriquecimento de dados:

Comunicação por voz e texto
Tempo real, história Arquivos
No dispositivo, acesso a serviços online
Conexões sociais multidimensionais
Redes sociais, contatos, histórico de comunicação.
Microfone, Câmera, GPS.
Grande armazenamento local
Poder de computação forte no dispositivo
Sempre ligado e conectado à Internet
Exfiltered on demand, envie comandos

- Interceptação nas comunicações
- Rede, homem no meio, no celular, empresa de celular

- Rastreamento de localização
- GPS, Rede, empresa de celular

- Extração de dados físicos
- Perda, roubo

- Fator humano
- Engenharia social aproveitando o uso extremo

- Cavalos de tróia
- Distribuição dirigida e massiva

- Aplicativos
- Malware, vazamento de dados

KAYMERA
Mobile security redefined

Citadel - Brasil

1- Interceptação de comunicação de voz e de dados

Interceptação de comunicação de voz e de dados é uma das maiores ameaças a que estão sujeitos os dispositivos móveis e esta interceptação pode ser executada de várias e diferentes maneiras.

1.1 - No nível do operador de rede

O operador de rede tem habilidade para interceptar e gravar qualquer comunicação em sua infraestrutura de rede. Esta informação pode ser acessada posteriormente tanto pelos funcionários do operador como por agências do governo com acesso próprio. O controle da rede neste nível pode ser usado para interceptar voz, texto e comunicação de dados, assim como localizar uma pessoa com base na triangulação da torre de celular. Em viagem ao exterior, qualquer chamada, comunicação por texto ou dados podem ser interceptadas pelo operador local e usadas com o propósito de coletar informações e fazer espionagem comercial.

1.2 - " Homem no meio" - BTS, Wi-Fi

Uma maneira efetiva de interceptação de voz, comunicação por texto e dados é utilizar os detectores de IMSI. O detector de IMSI é na verdade uma torre de celular falsa controlada pelo atacante mascarando-a como parte legítima da rede. A torre falsa usa um sinal bastante forte em proximidade com o celular da vítima para forçar o dispositivo a conectá-la e serve com ponto intermediário entre o telefone e a rede legítima. O detector IMSI pode interceptar voz, SMS e em alguns casos comunicação de dados.

Um ataque MitM com base em Wi-Fi pode ser facilmente orquestrado através de um cartão de rede sem fio pronto para uso conectado a um laptop com apenas alguns aplicativos. Neste ataque MitM com base em Wi-Fi, o atacante configura uma rede de Wi-Fi falsa que se disfarça como legítima (normalmente enquanto bloqueia a rede original) e atrai a vítima para conectá-la. Outra opção é o atacante escanear o dispositivo da vítima por uma rede Wi-Fi previamente armazenada e uma vez identificada, configura a rede falsa com o mesmo nome e características da rede original. A comunicação de dados da vítima pode então ser facilmente monitorada e manipulada pelo atacante.

2 - Ataques de Tróia

Os Cavalos de Tróia podem ser escondidos em aplicativos que parecem legítimos; eles podem também ter acesso aos smartphones com a ajuda de sistemas avançados, possibilitando ataques localizados a alvos selecionados com base em uma variedade de opções para infecção, incluindo aquelas que não requerem nenhuma interação ou envolvimento do usuário final.
Estes ataques remotos e ocultos possibilitam extração de dados totalmente não rastreáveis do dispositivo infectado e controle total dos recursos do dispositivo incluindo microfone, câmera, serviços, canais de comunicação, conexão com a internet, etc. Estes Cavalos de Tróia, uma vez instalados e ativos podem executar a coleta de informações militares de ponta e operações de vigilância pelo vazamento de informações e de dados armazenados no dispositivo, escutas não autorizadas, comunicação de dados (desta forma evitando qualquer criptografia que possa existir), fazendo a localização e rastreamento em tempo real, operando furtivamente o microfone dos smartphones e também a câmera, simulando informações geradas no dispositivo em lugar do usuário (mensagens de texto, e-mails, etc), somente para listar algumas opções. Infectar um smartphone com um Cavalo de Tróia é considerado o “Santo Graal” das operações de inteligência, já que smartphones são considerados o “máximo” em coleta de informações.

3 - Acompanhamento de localização

Como sempre levamos nossos Smartphones conosco, eles podem ser facilmente usados como dispositivos de rastreamento por um invasor comum. O chip GPS embutido pode ser empregado por qualquer aplicativo ou por um cavalo de Tróia com os direitos de acesso corretos para rastrear a localização de alguém em tempo real. Nos casos em que um sinal de GPS não pode ser obtido por algum motivo (má recepção, restrição no dispositivo, etc.), a leitura WiFi e alguns serviços de rede disponíveis podem ser usados para fornecer um local mais grosseiro ainda que utilizável. Além disso, a conexão do telefone com a rede celular pode ser explorada para identificar a localização de uma pessoa usando triangulação de torre de celular simples, mas altamente precisa, no nível do operador de rede. Existem vários serviços comerciais que oferecem serviços de triangulação celular em todo o mundo usando o número de telefone ou um dos identificadores exclusivos do telefone (IMSI e IMEI).

4 - Aplicativos

Os usuários confiam em aplicativos para melhorar a funcionalidade de seus smartphones, mas essa funcionalidade extra às vezes tem um preço para privacidade e segurança. Com os usuários gastando 85% de seu tempo em smartphones usando aplicativos e o usuário médio acessando 30 novos aplicativos por mês, os invasores estão se alinhando para aproveitar o extremo comportamento do usuário e os vastos requisitos de funcionalidade para obter acesso ilegal a informações, dados e recursos de smartphone. Existem basicamente dois tipos de aplicativos arriscados:

4.1 – Vírus: desonesto por natureza

Essas aplicações foram projetadas com um objetivo malicioso em mente. Eles podem conter um cavalo de Tróia como parte de seu pacote de instalação ou servir como cavalo de tróia ("com uma licença" - baixados, instalados e com permissões de usuários finais). Eles geralmente se mascaram como aplicativos legítimos, mas têm um propósito específico de obter acesso ilegal a dados, informações e recursos e usarão várias técnicas para convencer o usuário a fazer o download e instalá-los em seu dispositivo. Em um ataque orquestrado, isso pode ser uma mensagem falsa de um amigo recomendando o aplicativo ou alguma explosão de mensagem direcionada (ofertas gratuitas de uma rede ou de um provedor de serviços, por exemplo).

4.2 - Aplicativos Legítimos Acessando Recursos

Apps legítimos geralmente pedem ao usuário acesso a muito mais recursos do que os aplicativos realmente precisam para fornecer suas principais funcionalidades e objetivos de design. Por exemplo, um simples aplicativo de lanterna que precisa acessar apenas o flash da câmera para fornecer sua funcionalidade principal também pode solicitar o acesso a segmentos de dados adicionais e recursos, como serviços de localização ou contatos durante o processo de instalação.

O aplicativo usa esses recursos ou dados adicionais para fins de monetização. O usuário, ao instalar o aplicativo, geralmente sem estar ciente das consequências de suas ações, concede automaticamente acesso a dados e recursos extensos.

4.3 – Localização geográfica

Como nós tendemos a carregar nossos smartphones conosco todo o tempo, eles podem facilmente ser usados como instrumento de rastreamento por um atacante habitual. O chip de GPS integrado pode ser usado por qualquer aplicativo ou por um Cavalo de Troia com acesso para rastreamento de localização em tempo real. Em casos onde o sinal do GPS não pode ser obtido por qualquer razão (recepção ruim, restrição do aparelho, etc) a leitura do Wi-Fi com algum serviço de rede disponível pode ser usada para fornecer uma localização usável, ainda que grosseira. Além disso, a conexão à rede do celular pode ser usada para obter a localização de alguém utilizando a triangulação de uma torre de celular simples mas com resultado preciso. Há vários serviços de triangulação de celulares que são oferecidos em todo o mundo usando o número de telefone ou um dos identificadores do aparelho (IMSI e IMEI).

5 - Implicações dessas ameaças e técnicas de coleta de informações

À luz dos riscos descritos e com o objetivo de criar um ambiente seguro para o uso dos smartphones, deveríamos ter em mente as seguintes dicas:

5.1 – Cobertura para ameaças e proteção abrangente

Uma vez que os atacantes podem utilizar diversos métodos para atingir seus objetivos e também há várias técnicas de coleta de informações disponíveis, a solução seria adotar uma abordagem holística na segurança do aparelho.

5.2 - Seja o mais transparente possível
Proporcione máxima funcionalidade

Levando em consideração que a maioria dos usuários de smartphones não tolera as restrições, não há regras de segurança estabelecidas por políticas de restrição. Na verdade, se você eliminar alguma das funcionalidades do smartphone, como instalar aplicativos de sua escolha, o uso das redes sociais, o surfing na web, o uso de câmera e serviços de localização ou a comunicação livre com outras pessoas, você poderia, com certeza, criar um ambiente seguro. Entretanto, isto privaria os smartphones de serem “smart”. Para criar um equilíbrio entre segurança e usabilidade, a segurança precisa ser construída no smartphone original em oposição a ser colocada como um aplicativo ou serviço.

KAYMERA
Mobile security redefined

Citadel - Brasil

- Fornece uma plataforma de defesa móvel cibernética altamente flexível, apoiada por uma infraestrutura de comunicação e gerenciamento de conteúdo seguro em vários níveis.
- Detecta, evita e protege contra qualquer ameaça móvel.
- Permite mobilidade ao abordar várias necessidades de segurança móvel em vários segmentos de funcionários.
- Mantém um equilíbrio ideal em segurança, funcionalidade, uso e produtividade de primeiro nível.

KAYMERA
Mobile security redefined

Citadel - Brasil

CIPHERBOND
Secure Communication

CIPHERWATCH
Adapted Mobile Threat Defense

KAYMERA SECURE DEVICE

Android-based, pronto para uso

KAYMERA
Mobile security redefined

Citadel - Brasil

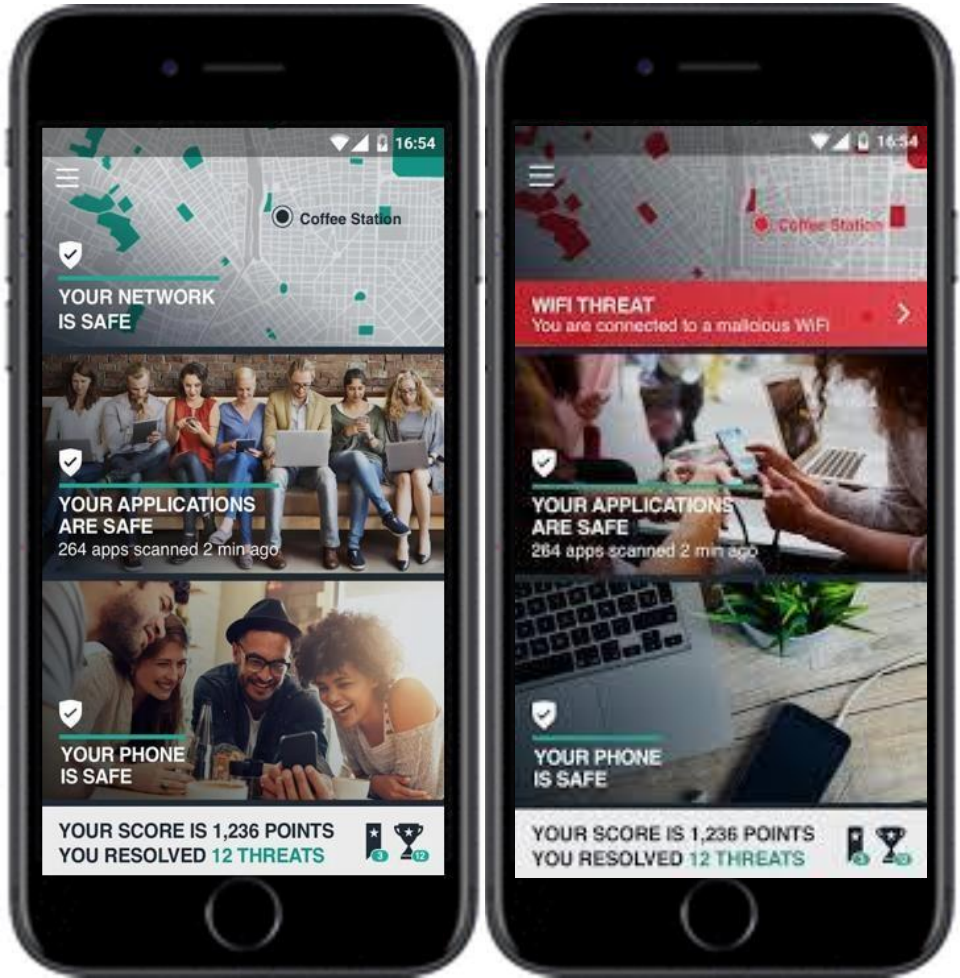
CIPHERWATCH - ADAPTED MOBILE THREAT DEFENSE

DETECÇÃO DE ALERTAS **BASEADA NA REDE**

- Conexão insegura (Wi-Fi / Dados Móveis)
- Rogue Access Point
- Ataque Wi-Fi Man-In-The-Middle:
- ARP Spoofing
- Divisão SSL

DETECÇÃO DE ALERTAS BASEADA **NA LOCALIZAÇÃO**

- Áreas restritas usando balizas BT
- Regiões de alto risco



KAYMERA
Mobile security redefined

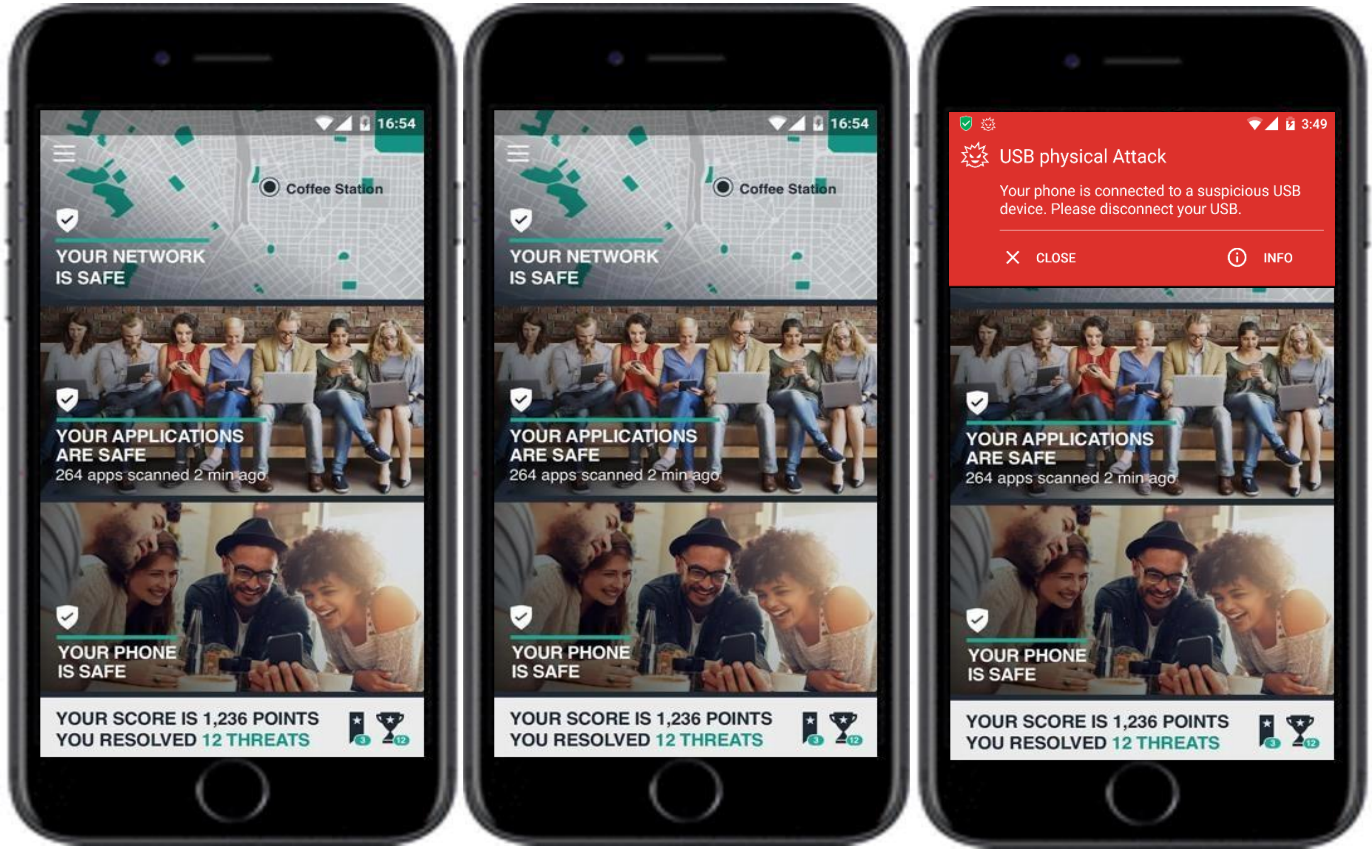
Citadel - Brasil

DETECÇÃO DE ALERTAS BASEADO **NO DISPOSITIVO**

- Jailbreak/Root
- Versão de OS
- Encriptação de dados
- Proteção de senhas
- Status do modo de desenvolvedor
- ADB habilitado
- Fontes desconhecidas ativadas
- Tempo limite da tela de bloqueio
- Dispositivo comprometido com rede de segurança
- Ameaças por USB

SCANNING DE APLICATIVOS

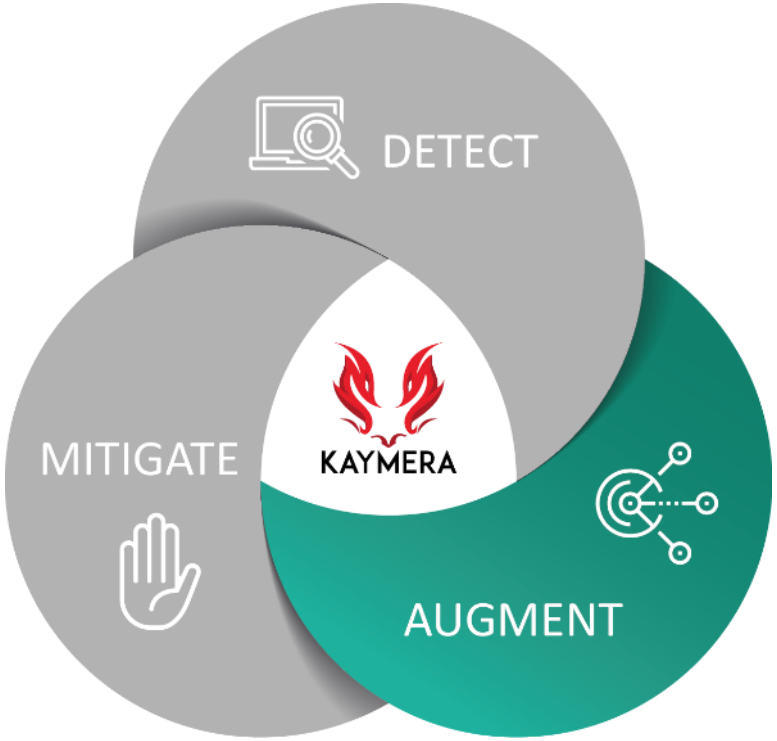
- Reputação de aplicativos instalados
- Análise estática de aplicativos
- Análise dinâmica de aplicativos instalados
- Aplicativo desconhecido ou reempacotado

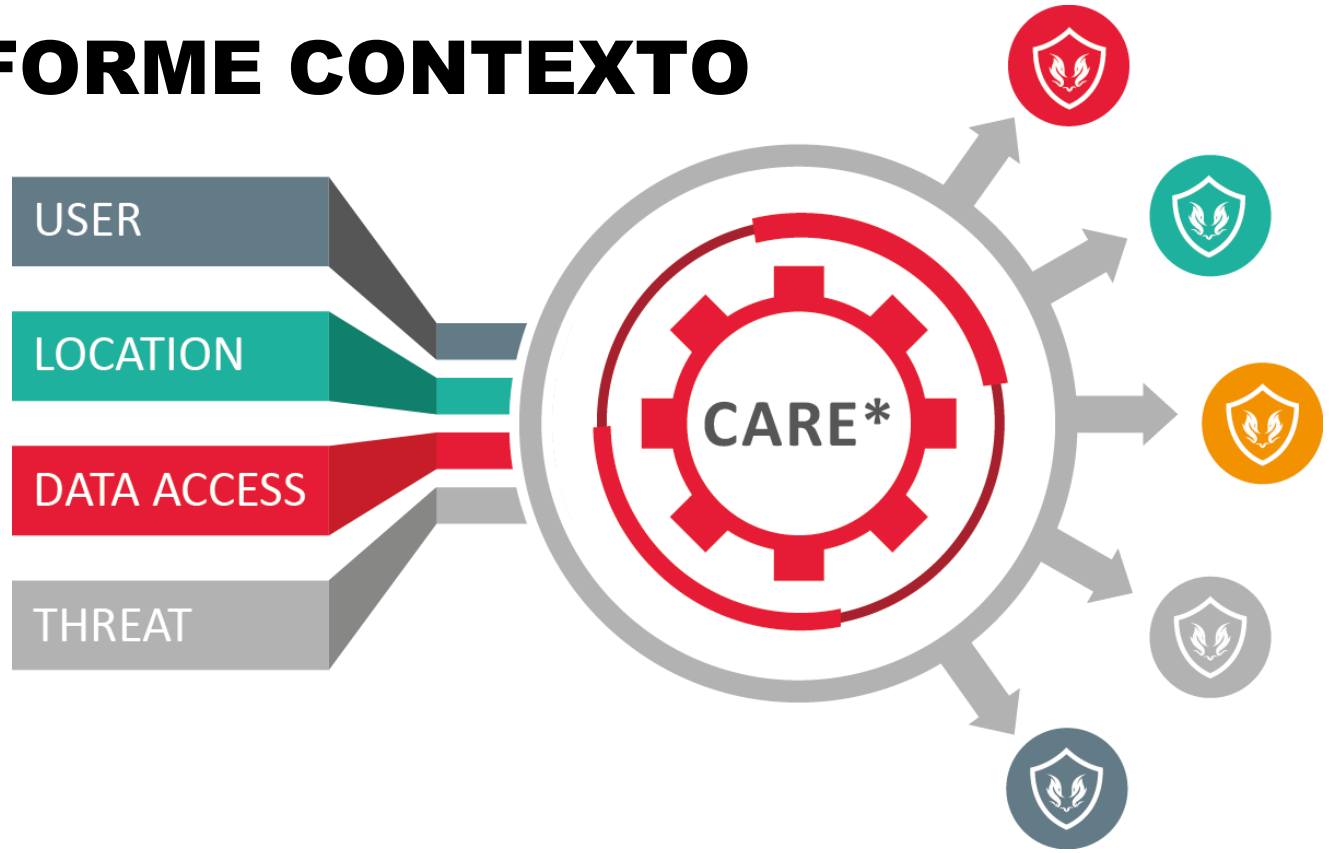


KAYMERA
Mobile security redefined

Citadel - Brasil

ANÁLISE DE RISCO CONFORME CONTEXTO

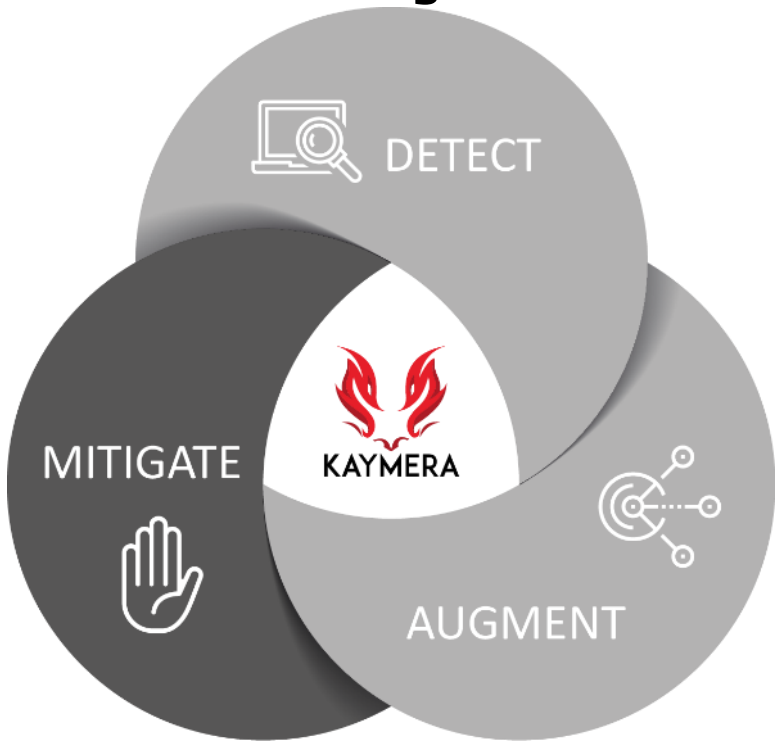




KAYMERA
Mobile security redefined

Citadel - Brasil

ORQUESTRAÇÃO E MITIGAÇÃO



O CipherWatch protege dispositivos gerenciados e não gerenciados.

MITIGAÇÃO DE EMM GERENCIADO

airwatch

MobileIron

KAYMERA MDM

- Os próprios recursos de MDM Kaymera
- Conexão segura de dados via VPN por risco

MITIGAÇÃO NÃO GERENCIADO (NO MDM)

- MS Email (Exchange) server
- Cloud services: Office 365, CASB
- APIs de aplicativos da empresa

Active Directory

Office 365

Exchange

KAYMERA
Mobile security redefined

Citadel - Brasil

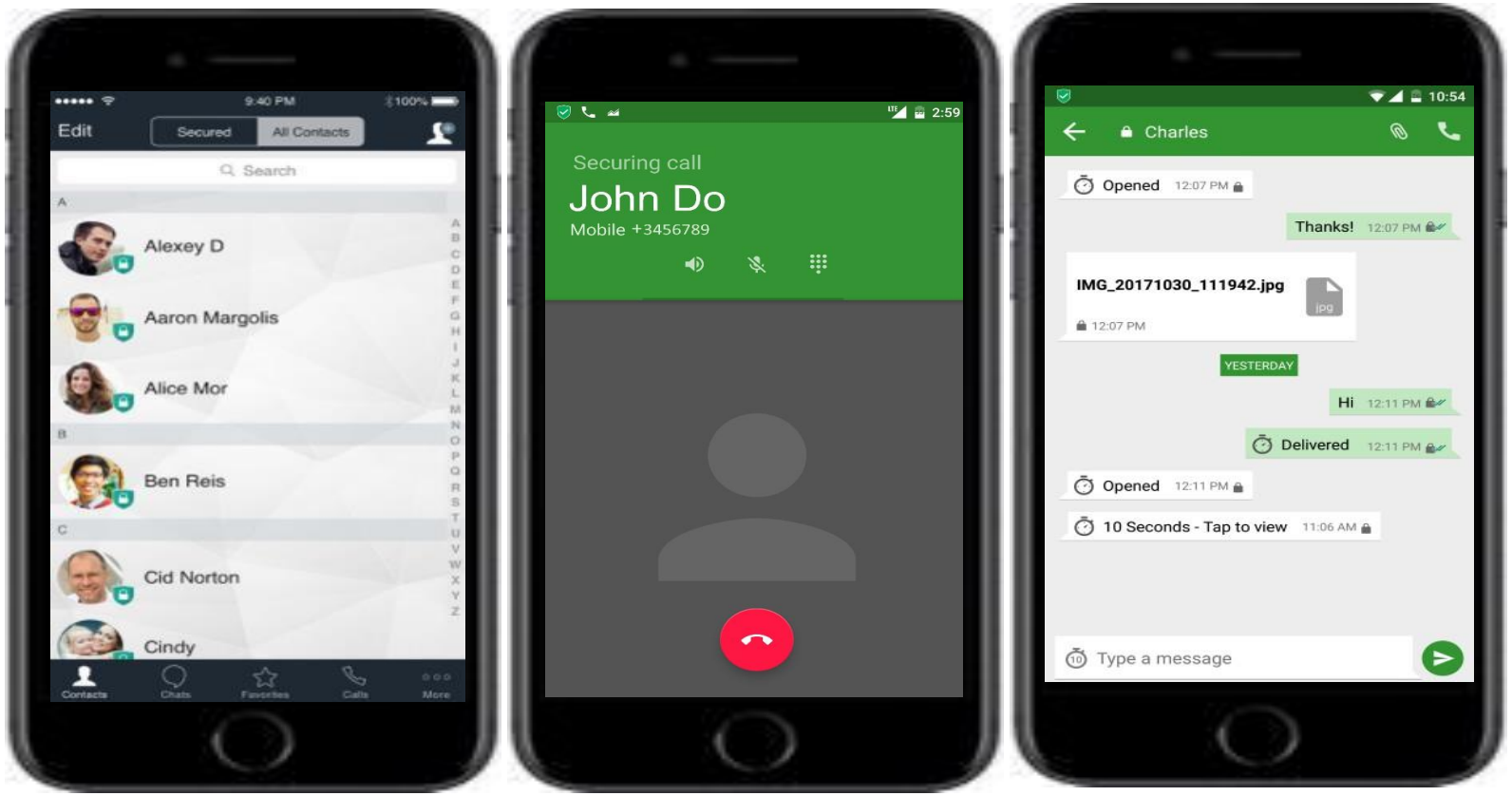
CIPHERBOND – COMUNICAÇÃO MÓVEL SEGURA

VOZ

- Chamadas seguras de ponta-a-ponta;
- Chamadas seguras usando o número de contato;
- Chamadas seguras em conferência.

MENSAGEM DE TEXTO

- Criptografia de ponta-a-ponta;
- Chats de grupos seguros;
- Mensagens autodestrutivas;
- Compartilhamento seguro de mídias e arquivos.



KAYMERA
Mobile security redefined

Citadel - Brasil

Solução CipherFort

Esta seção descreve a solução de segurança CipherFort e suas características.

1 - KAYMERA OS - O usuário final do aparelho

O aparelho do usuário final teria como base o KAYMERA OS, um sistema de operações altamente seguro, feito da base ao topo para maximizar a proteção do aparelho com os mais altos padrões de utilidade, conforme fornecido pela plataforma Android.

1.2 – A proteção do aparelho

A camada de proteção é responsável por proteger o aparelho contra infestação por vírus e acesso remoto não autorizado através de interfaces disponíveis, além de proteger fisicamente os dados do smartphone.
O aparelho é protegido de todos os ataques conhecidos, incluindo:
Interceptação de rede: as comunicações por voz, SMS e internet estão protegidas.
Wi-Fi: protegido contra interceptação, manipulação de dados e infestação.
Extração de dados: protegido contra extrações físicas.
Cavalos de Tróia e ataques de vírus: política de controle de permissão total sobre OS.

1.3 - Camada de proteção

Esta é uma proteção que evita que processos que estejam rodando no sistema sejam acessados por fontes não autorizadas. É usada como uma rede de proteção em casos onde o código malicioso tiver a possibilidade, de alguma forma, de burlar a camada de proteção e ser executado no sistema seguro. É também usado para monitorar o comportamento dos processos autorizados e aplicativos e evitar que sejam acessados sem autorização no momento da execução.

1.4 - Camada de detecção de riscos

Quando o aparelho está sob ataque ou em ambiente inseguro, alertas em tempo real irão notificar o usuário pelo celular, com uma sugestão opcional de mitigação. Isto permitirá ao usuário identificar quando seu aparelho estiver sob ataque e agir de acordo com a necessidade.
Esta camada detecta anomalias no dispositivo e também as anomalias que possam afetar a rede. Juntamente com um sofisticado sistema analítico no dispositivo, esta camada pode avaliar riscos em tempo real e aplicar políticas de segurança rigorosas. As sondas de detecção estão incluídas no Kaymera OS e usadas para determinar o risco e identificar ataques cibernéticos em tempo real.
A integração das soluções SOC e SIEM está disponível como item opcional através de KAYMERA API.

1.5 - Segurança pessoal

A solução Kaymera CipherFort foi desenhada para proteger as comunicações e informações confidenciais do usuário mesmo em face de encontro físico com uma terceira parte não amigável. Para dar apoio nesta situação, um sofisticado Módulo de Pânico foi implementado como parte do sistema operacional de segurança, no qual os usuários podem silenciosa e veladamente proteger seus dados e ao mesmo tempo relatar à sede em tempo real um caso no qual sejam forçados a entregar e desbloquear o dispositivo Kaymera para inspeção física.

1.6 – Comunicação segura integrada

Criptografia de ponta a ponta para chamadas, textos, chats e compartilhamento de arquivos entre usuários de Kaymera com nível de criptografia AES 256-bit. As chaves da criptografia são geradas e guardadas somente no hardware do dispositivo, no conjunto de circuitos integrados protegidos Keystore.

KAYMERA
Mobile security redefined

Citadel - Brasil

1.7 – Maximizando o uso

O Kaymera OS está disponível em um conjunto de dispositivos de alta qualidade. Modelos de apoio atuais:
Google Pixel 2 / Pixel 2XL

O Kaymera OS tem os mais altos padrões de usabilidade e possui as últimas versões da plataforma Android OS. Kaymera OS lhe permite:

- Armazenar a experiência Android sem aplicativos pré-instalados
- Suporte para as últimas versões através das atualizações do OTA (Secured Off-the-Air) do Kaymera.

Google Pixel 2 XL com KAYMERA OS

KAYMERA
Mobile security redefined

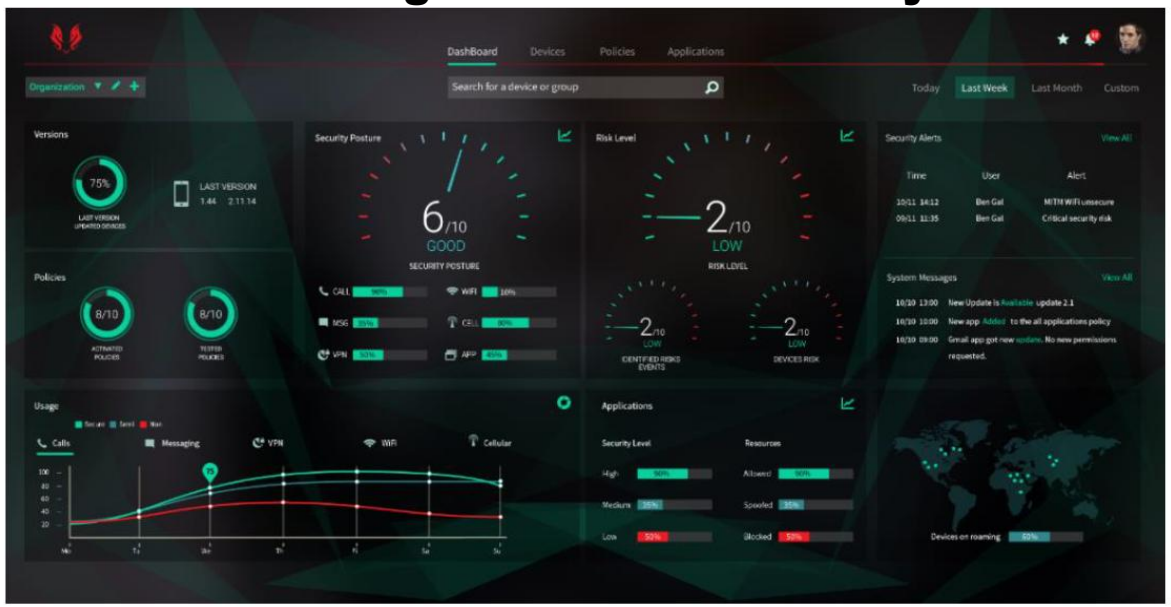
Citadel - Brasil

2 – Painel de controle do KAYMERA

O aplicativo de gerenciamento do Kaymera permite aos gerentes de TI e de Segurança um completo controle sobre o ambiente dos aparelhos dos usuários finais com o propósito de garantir a segurança dos dispositivos, incluindo:

- Sistema de gerenciamento do painel com apoio do multi-tenancy
- Monitoramento de rede e gerenciamento do aparelho
- Aplicação das políticas de risco da organização
- Geração de relatórios

Interface de gerenciamento do Kaymera



KAYMERA
Mobile security redefined

Citadel - Brasil

Principais Benefícios:

- Poderosa detecção de ameaças em tempo real;
- Análise de risco em tempo real sensível ao contexto;
- Eliminação de ameaças automatizada;
- Suporte para BYOD (Uso de dispositivo próprio) / CYOD (Dispositivo fornecido pela empresa);
- Aumento dos índices de adesão dos funcionários, mantendo sua privacidade com detalhamento da eliminação de riscos não gerenciada,
- Integração fácil com estruturas de TI pré-existentes.

Os recursos do sistema incluem:

- Aplicação de segurança para acesso remoto;
- Recursos de adaptação;
- Acesso remoto;
- Distribuição de licença e versão do sistema,
- Gerenciamento de senhas.

Abordagem multicamada de Defesa

Citadel - Brasil

Encriptação

Dados em repouso, dados em movimentos. Comunicação segura de dados, voz e texto.

Proteção

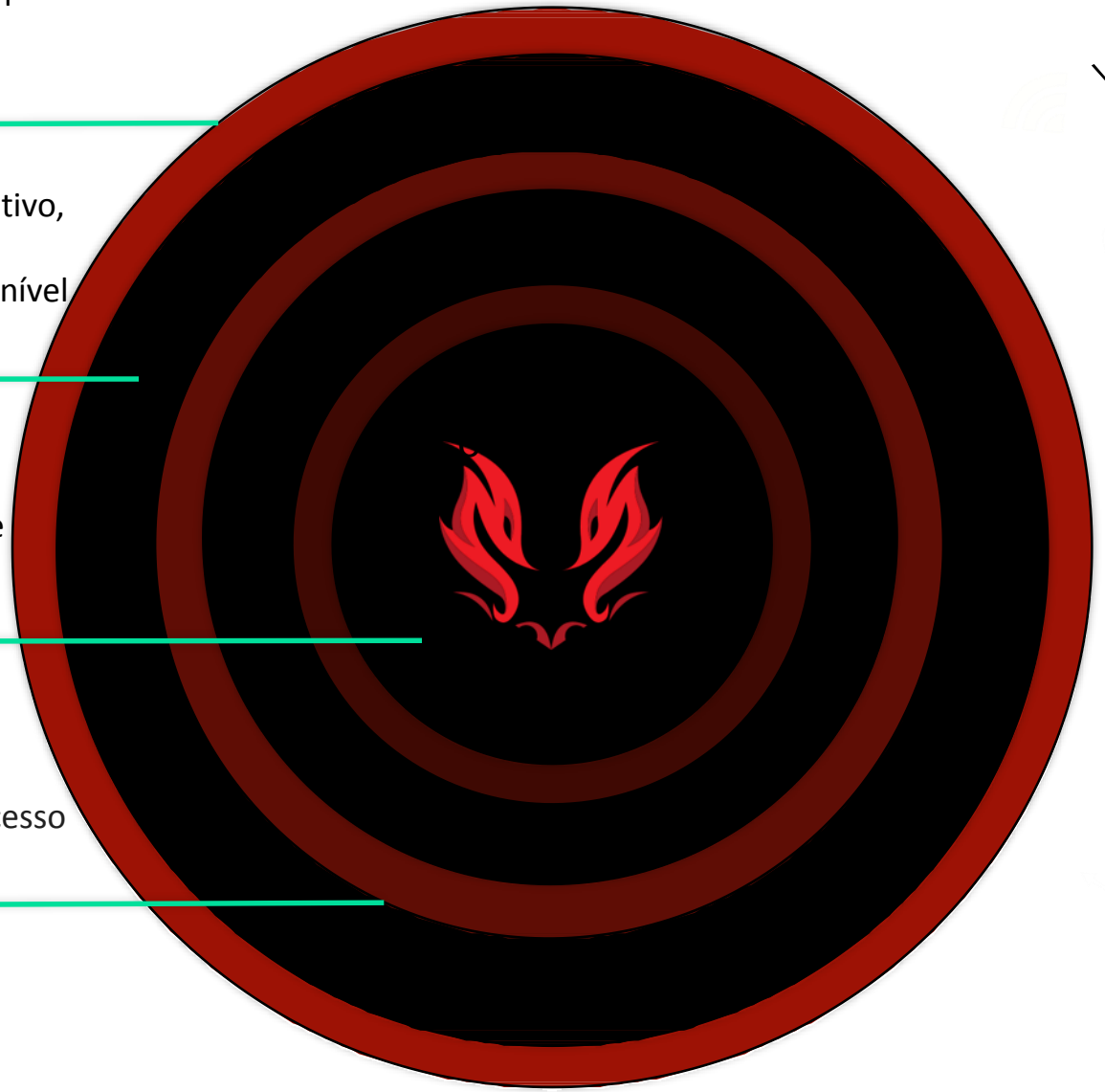
Evita a exploração de interfaces externas, a penetração do dispositivo, o controle de acesso físico, o endurecimento do dispositivo no nível do controlador.

Prevenção

Impede o acesso não autorizado a recursos do dispositivo em caso de malware ou aplicativo desonesto.

Detecção

Ataques de rede e ambientais, acesso físico e anomalias no celular.



Wi-Fi

Sesiones Web

Apps

Bluetooth

Red Celular

USB


KAYMERA
Mobile security redefined
Citadel - Brasil
CITADEL
Citadel-Security & Intelligence Solutions LTD.
www.citadel-brasil.com
Email: aschmoisman@citadel-brasil.com
Mobile: +55 11 98971 2194
Augusto Schmoisman