Serviço de proteção completa
contra ciberameaças

Kaspersky Digital Footprint Intelligence

kaspersky bring on the future

Perguntas para os especialistas

Qual a melhor maneira de lançar um ataque contra sua organização?

Qual a maneira com melhor custo-benefício para atacar você?

Quais informações estão disponíveis para um invasor que tenha sua empresa como alvo?

Sua infraestrutura já foi comprometida sem seu conhecimento?

O Kaspersky Digital Footprint Intelligence responde a essas e outras perguntas, enquanto nossos especialistas montam um panorama abrangente do seu status de ataque, identificando pontos fracos para exploração e revelando evidências de ataques passados, presentes e até planejados.

Introdução

À medida que a sua empresa cresce, a complexidade e a distribuição dos seus ambientes de TI crescem também, criando um desafio: proteger sua presença digital amplamente distribuída sem controle direto ou propriedade. Ambientes dinâmicos e interconectados permitem que as empresas obtenham benefícios significativos. No entanto, a interconetividade em constante crescimento está também expandindo a superfície de ataque. À medida que os invasores se tornam mais habilidosos e competentes, é vital não apenas ter uma visão completa da presença online de sua organização, mas também ser capaz de rastrear suas mudanças e reagir a ameaças externas direcionadas a quaisquer bens ou materiais digitais expostos.

As organizações usam uma gama de ferramentas de segurança em suas operações de segurança, mas ainda existem ameaças digitais que exigem recursos muito específicos - para detectar e mitigar vazamentos de dados, monitorar planos e esquemas de ataque de cibercriminosos em fóruns da dark web etc. Para ajudar os analistas de segurança a explorar a visão do adversário sobre os recursos de sua empresa, descobrir os possíveis vetores de ataque a tempo, e ajustar suas defesas de acordo, a Kaspersky criou o Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence fornece

O Kaspersky Digital Footprint Intelligence é um serviço completo de proteção contra riscos digitais. Com ele, os clientes podem monitorar seus materiais digitais e detectar ameaças da Web comum até as profundezas da dark web.

Reconhecimento de rede

Identificação dos recursos de rede do cliente e serviços expostos que são um potencial ponto de entrada para um ataque. Análise personalizada das vulnerabilidades existentes, com pontuação e avaliação de risco abrangente adicionais baseadas na pontuação base do CVSS, disponibilidade de exploits públicos, experiência de testes de penetração e localização do recurso da rede (hospedagem/infraestrutura).

Monitoramento da Dark Web

Monitoramento contínuo de dezenas de domínios da Dark Web (fóruns, blogs de ransomware, messengers, websites tor, e etc.) para detectar quaisquer referências e ameaças relacionadas à sua empresa, clientes e parceiros. Análise de campanhas ativas de ataque direcionado ou ataques que estejam sendo planejados, campanhas de APT direcionadas para à sua empresa, setor ou região de operações.

Descoberta de vazamentos de dados

Detecção de dados comprometidos de colaboradores, credenciais de parceiros e clientes, cartões bancários, números de telefone e outras informações confidenciais que podem ser usadas para perpetrar um ataque ou podem representar riscos para a reputação da empresa.

Detecção de ameaças

Monitoramento de atividades fraudulentas que podem prejudicar a reputação de uma empresa e/ou decepcionar os clientes.

Suporte para multilocação

Recursos incrementados para provedores de serviços de segurança gerenciada (MSSPs) e organizações de grande porte com estrutura de filiais.

Como funciona

Configuração	Coleta	Resposta	Filtro
Descoberta de informações sobre ativos digitais da empresa	Coleta automatizada de dados da internet, deep e dark webs e da base de conhecimento Kaspersky	Fornecimento de notificações sobre ameaças operacionais no Portal Kaspersky Threat Intelligence via API	Detecção, análise e priorização de ameaças gerenciadas por analistas

Principais resultados a se esperar do serviço

1. Painéis úteis com estatísticas detalhadas
2. Cota de pesquisa no banco de dados da dark web
3. Alertas de ameaças no Threat Intelligence Portal
4. Cota de pesquisa no banco de dados de redes sociais
5. Seminários e sessões de perguntas e respostas com especialistas
6. Dados legíveis por máquina
7. Relatórios analíticos compilados por nossos especialistas*
8. Solicitações de remoção de domínios e recursos da Web (Takedown)*

*Serviço de complemento

Tipos de ameaças

O Kaspersky Digital Footprint Intelligence capacita as organizações a reagirem de forma rápida e eficiente contra ameaças potenciais, por meio de alertas em tempo real. A solução reduz a probabilidade de danos contra a reputação de empresas, confiança do cliente e das operações comerciais em geral. As empresas podem personalizar os recursos de monitoramento do serviço para atender às suas necessidades específicas, além de relatórios e análises abrangentes que oferecem insights valiosos sobre o escopo e o impacto da violação de marca e outros riscos potenciais.

Ameaças relacionadas ao perímetro da rede

- Serviços de rede configurados incorretamente
- Identificação de vulnerabilidades
- Recursos modificados ou comprometidos

Ameaças relacionadas à dark Web

- Esquemas de fraudes e planos de agentes cibercriminais
- Venda de violação de dados
- Atividades de insiders

Vazamentos de dados

- Recursos corporativos comprometidos
- Cartões de crédito comprometidos
- Credenciais comprometidas

Ameaças relacionadas a malware

- Ataques de phishing
- Ataques direcionados
- Campanhas de APT

Fontes de inteligência

É fundamental que nossos clientes adquiram uma compreensão abrangente da sua postura de segurança externa. Para fornecer essas informações, os analistas de segurança Kaspersky coletam e agregam informações extraídas das seguintes fontes de inteligência:

Seus dados não estruturados

- Endereços de IP
- Domínios da empresa
- Nomes de marcas
- Palavras-chave
- Alcances de rede
- Números de cartão BIN/IIN
- Informações de funcionários

Inventário de perímetro de rede

Busca de superfície, deep e dark web

Busca na Base de Conhecimento da Kaspersky

Alertas de ameaças

Pesquisa em tempo real pelos recursos da Kaspersky, Internet e Dark Web

Solicitações de remoção de domínios e recursos da Web (Takedown)*

Relatórios analíticos*

Recursos de execução de serviços

Os recursos avançados de Digital Footprint Intelligence para provedores de serviços gerenciados (MSSPs) e organizações de grande parte com estrutura de filiais.

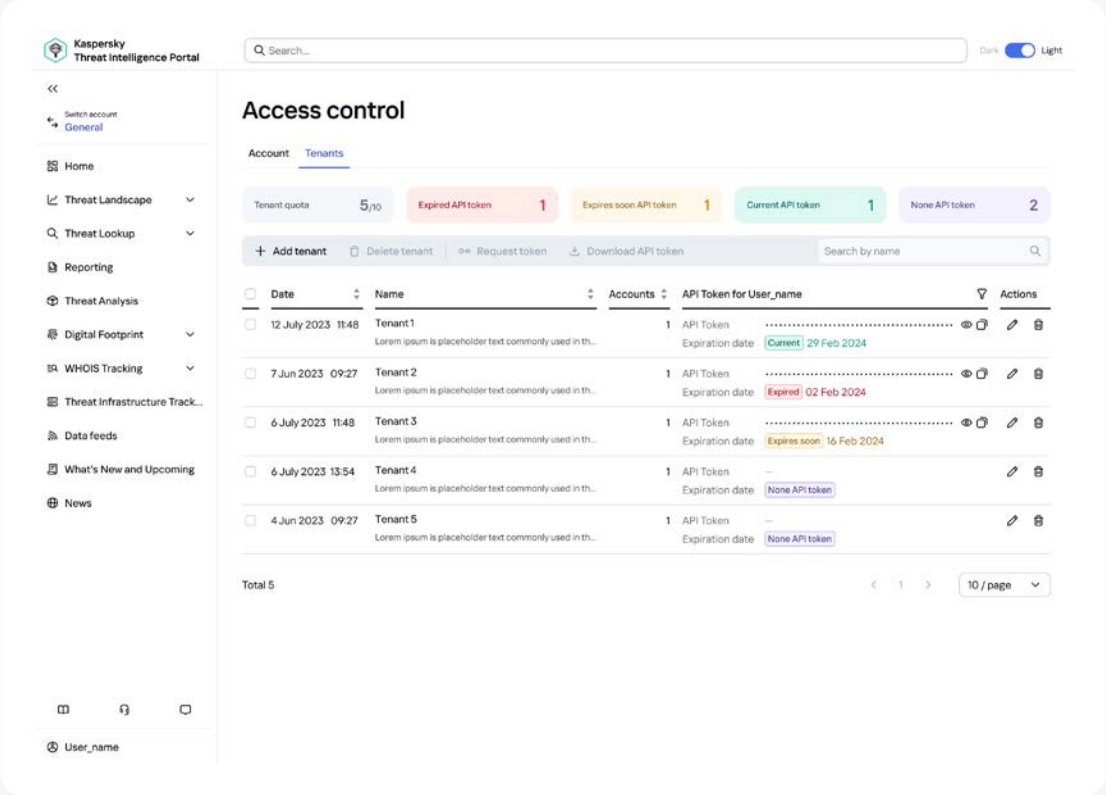
A interface do Kaspersky Threat Intelligence Portal que fornece o serviço DFI permite aos MSSPs obterem acesso diferenciado a informações relacionadas às subsidiárias de organizações de grande porte ou a organizações individuais para as quais eles fornecem serviços gerenciados de segurança.

Criação de tenants separados e configuração de controle de acesso via painel de administração

O gerenciamento é feito através da criação de tenants, que são entidades lógicas criadas para cada nova estrutura, gerenciadas separadamenteuma das outras.

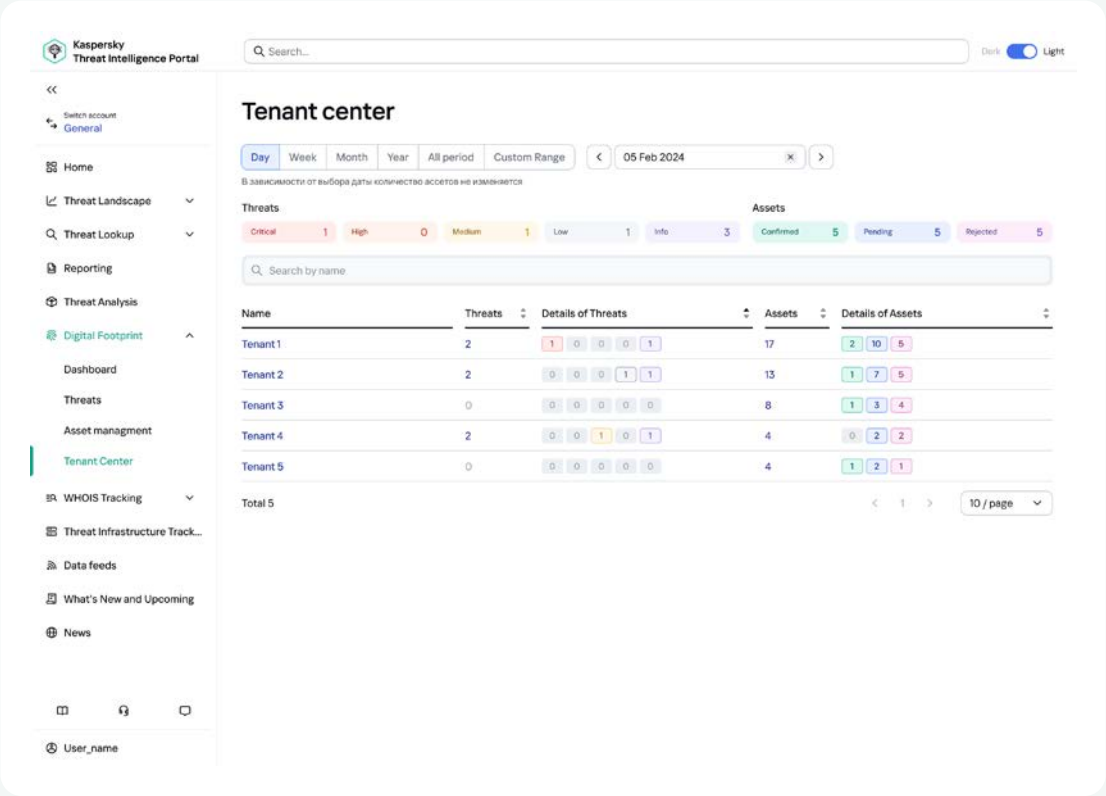
1. Acesso a todas as notificações de ameaças específicas de cada tenant e ativos
2. Alternância e visualização descomplicada de grupo de tenants para cada tenant
3. Controle de acesso por token de API e TOTP
4. Capacidade de alterar licenças de tenants

*Serviço de complemento



Estatísticas centralizadas sobre cada ameaça e ativo dos tenants

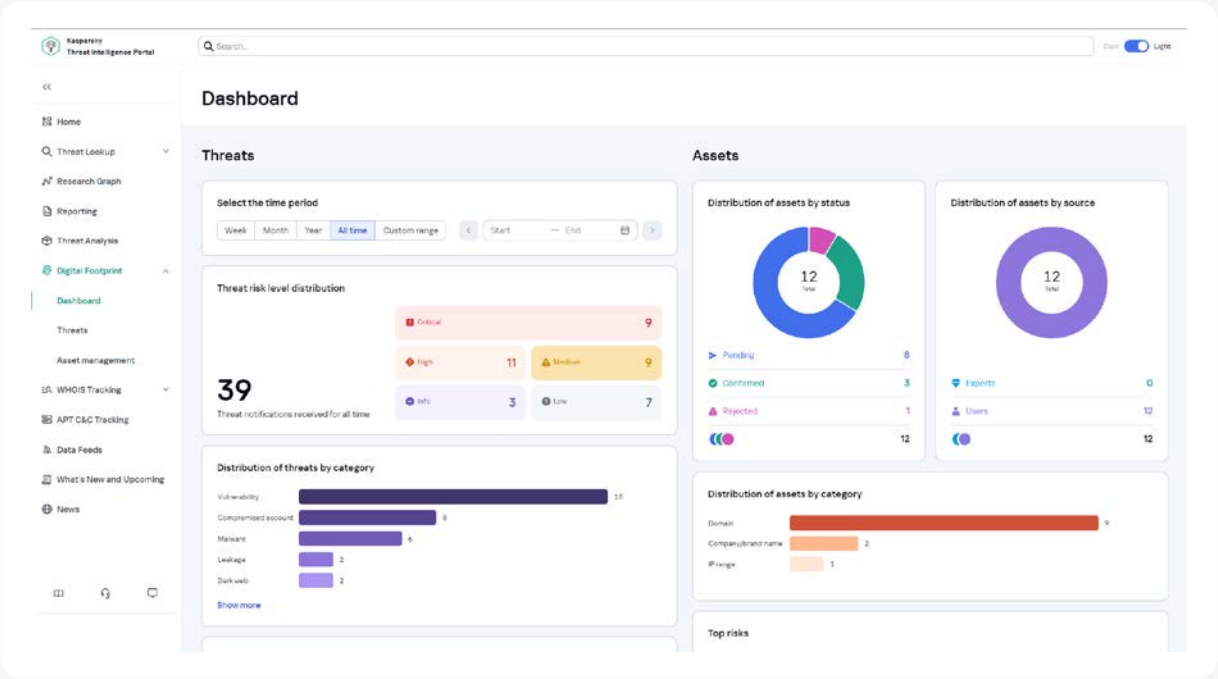
Ter a capacidade de fornecer o serviço para um grande número de organizações exige contar com ferramentas para monitorar o estado atual dos tenants. O Tenant Centar exibe um resumo para cada tenant, incluindo a quantidade de ameaças detectadas e seu nível de gravidade, bem como informações sobre os ativos que cada tenant gostaria de monitorar e seus status.



Monitoramento detalhado

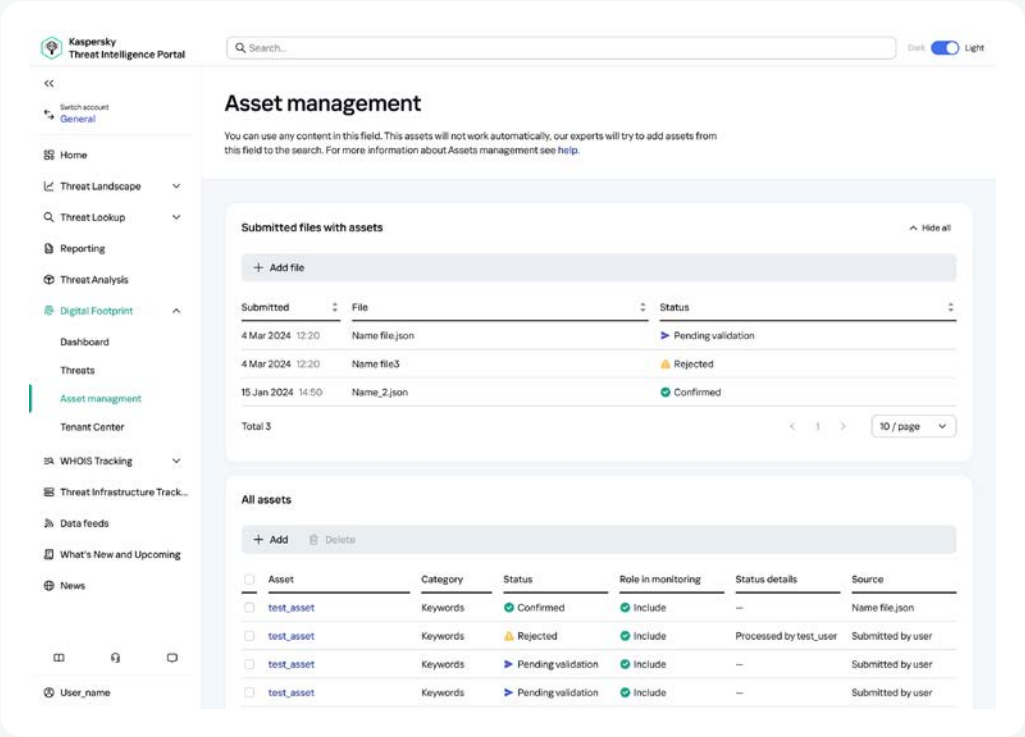
O MSSP ou o encarregado podem ver o resumo detalhado para cada tenant:

- Quantidade total de ameaças identificadas durante um determinado período e nível de gravidade para a organização
- Categorização de ameaças detectadas
- Os ativos de tenants mais vulneráveis
- Cenário de ameaças em constante mudança



Gerenciamento de ativos

O tenant é capaz de adicionar novos ativos para monitoramento ambos separadamente através da interface do Kaspersky Threat Intelligence Portal e também carregando arquivos com grande volume de ativos. Esta abordagem basicamente simplifica o processo de manter os ativos atualizados.



Valor comercial

O Kaspersky Digital Footprint Intelligence oferece benefícios e alto valor agregado para a sua organização:

Protege sua identidade

Detecte ameaças potenciais em tempo real e proteja a reputação da sua empresa, preservando a confiança dos clientes, reduzindo o risco de prejuízos financeiros e danos às operações comerciais.

Reduza os riscos cibernéticos

Equipe seus principais agentes (diretoria e gestão) com informações sobre onde concentrar os gastos com cibersegurança, expondo deficiências na configuração atual e os riscos que representam.

Reaja com agilidade

O contexto adicional para alertas de segurança aprimora a resposta a incidentes e reduz o tempo médio de resposta (MTTR).

Reduza sua superfície de ataque

Gerencie a presença digital da sua empresa e controle os recursos de rede externos para combater vetores de ataque e vulnerabilidades que podem ser usados em um ataque.

Entenda seus adversários

Prevenção e antecipação - saiba o que os cibercriminosos estão planejando e o que estão falando sobre a sua empresa na dark web e para que você possa estar preparado em caso de um ataque.

Domine o desconhecido

Melhore sua capacidade de resistir a ciberataques e de identificar ameaças fora do perímetro das equipes de segurança interna.

Eficiência na execução de serviços

Início rápido e fácil expansão no modo multi-tenant economiza tempo e dinheiro para os provedores de serviços gerenciados (MSSP) e seus clientes, bem como para as organizações afiliadas de grande porte.

Fale com nossa equipe para saber mais sobre os diversos planos de assinatura

Entrar em contato

Kaspersky Digital Footprint Intelligence

Saiba mais

www.kaspersky.com.br

© 2024 AO Kaspersky Lab.
As marcas comerciais registradas e as marcas de serviço pertencem aos seus respectivos proprietários.

#kaspersky
#bringonthefuture