
KASPERSKY lab
17:25:41
SOC powered by
Kaspersky Lab
www.kaspersky.com

Ao mesmo tempo que as empresas aprendem a se proteger melhor, os criminosos estão tramando técnicas ainda mais sofisticadas para transpor suas barreiras de segurança. Atraídos pelas oportunidades de ganhos sem precedentes que os ataques virtuais podem proporcionar, um número cada vez maior de agentes de ameaça buscam e miram ativamente as falhas de segurança não detectadas. Estão sendo criados mais centros de operações de segurança (SOCs, Security Operations Centers) para combater os problemas de segurança que surgem e dar uma resposta e uma solução rápidas.

"Os centros de operações de segurança devem ser planejados visando a inteligência, adotando uma arquitetura de segurança adaptável, sendo sensíveis ao contexto e orientados por informações. Os líderes de segurança devem entender como os SOCs orientados por informações usam ferramentas, processos e estratégias ***para se proteger contra as ameaças modernas."***

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, novembro de 2015

O SOC É UM DEPARTAMENTO CENTRALIZADO PARA O MONITORAMENTO E A ANÁLISE CONSTANTES DE AMEAÇAS, E TAMBÉM PARA A REDUÇÃO E PREVENÇÃO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA

Uma pesquisa recente realizada pela B2B International (publicada no final de 2016) com mais de 4000 empresas em 25 países descobriu que:

- **38%** dos participantes tiveram sérios **problemas com vírus e malware** nos 12 meses anteriores, o que gerou perda de produtividade.
- **21%** das empresas sofreram perda **de dados/exposição devido a ataques direcionados.**
- Cerca de 40% dos participantes destacaram esses desafios como preocupação específica.
- **17%** das empresas sofreram um **ataque DDoS** nos 12 meses anteriores, com frequência mais de uma vez.
- **42%** de todos os participantes da pesquisa que sofreram **ataques de phishing** eram empresas.
- **26%** de todos os eventos de **segurança passaram** despercebidos durante semanas ou mais, sendo revelados somente em auditorias de segurança externas.
- Nas empresas que sofreram pelo menos uma violação de dados, **o impacto financeiro médio** foi de **US$ 891 mil** (incluindo salários de pessoal interno, prejuízos em termos de avaliação de crédito/prêmios de seguros, perda de negócios, RP extra para reparar os danos à marca e contratação de consultores
- Esses números de **impacto** para as empresas **variaram de US$ 393 mil a US$ 1,1 milhão**, dependendo de quando a violação foi detectada – a rápida detecção gerou custos mais baixos para as empresas.
- O total de registros de clientes/funcionários suscetíveis comprometidos também variou de acordo com o tempo até a detecção – de 9 mil com detecção praticamente instantânea (havia um sistema de detecção) a 240 mil nos casos em que a violação não foi detectada por mais de um ano.

De acordo com o modelo de Arquitetura de Segurança Adaptável da Gartner, para ter sucesso no combate aos crimes virtuais no ambiente de ameaças atual, as equipes de SOC devem ser capazes de:

- PREVER
- DETECTAR
- PREVENIR-SE
- RESPONDER

Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014, Foundational January 2016

QUATRO ELEMENTOS PRINCIPAIS

Quatro elementos principais, combinados a processos claramente definidos e tecnologias relevantes, devem estar em vigor para sustentar essa abordagem reconhecida pelo setor. São eles:

- **GESTÃO DE CONHECIMENTO**. As pessoas (os integrantes das equipes de SOC) devem ter capacitação em perícia digital, análise de malware e resposta a incidentes para prevenir e responder bem a ataques cada vez mais sofisticados.
- **INTELIGÊNCIA DE AMEAÇAS**, obtida de várias fontes diferentes (quanto mais, melhor), é crucial para detectar ameaças em tempo hábil:
  1. Dados de ameaças internas
  2. Informações de fontes públicas (OSINT)
  3. CERTs do setor
  4. Fornecedores globais de antimalware
- **BUSCA POR AMEAÇAS** para pesquisar de forma proativa as ameaças que não estão sendo detectadas por sistemas de segurança tradicionais, como firewalls, IPS/IDS, SIEM, etc.
- **UMA ESTRUTURA DE RESPOSTA A INCIDENTES** implementada para limitar os danos e diminuir os custos de recuperação.

  Cada um desses elementos é igualmente importante e justifica uma atenção individualizada.

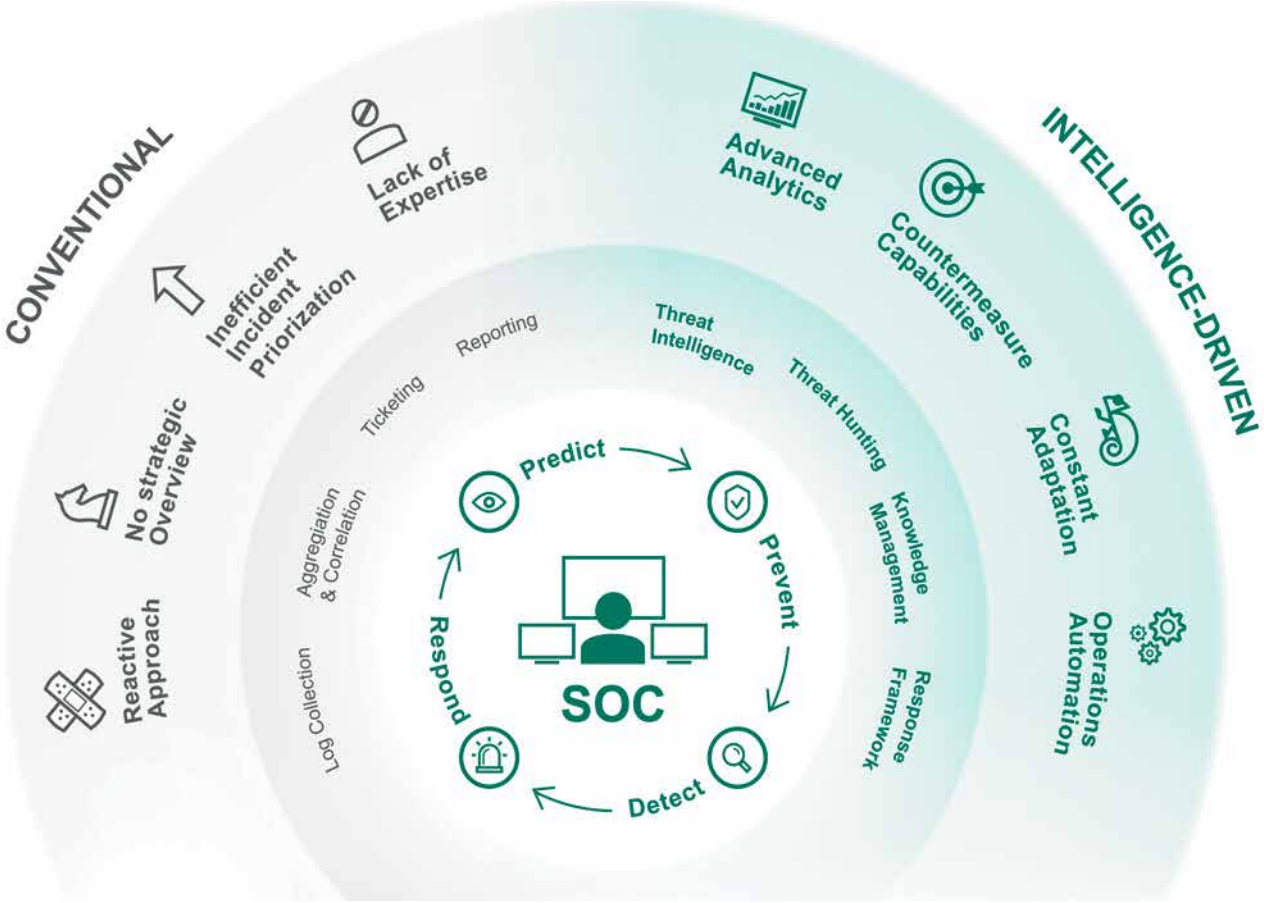


Figura 1:
Os quatro elementos principais do SOC.

GESTÃO DE CONHECIMENTO

O SOC deve fornecer um pool de recursos de conhecimento prático e experiência suficiente para analisar um imenso volume de dados e identificar onde é preciso aprofundar as investigações.

Os orçamentos limitados dificultam a alocação de pessoal para o SOC.

No momento, o mercado está carente de profissionais de segurança cibernética bem treinados, o que aumenta as despesas trabalhistas e de recrutamento.

Um membro eficiente da equipe de SOC deve:

- Ser curioso, capaz de elaborar um panorama geral da situação com base em fragmentos de dados dispersos.
- Ser capaz de manter a atenção contínua e, ao mesmo tempo, lidar com altos níveis de estresse.
- Ter bons conhecimentos gerais de TI e segurança cibernética, preferencialmente combinados a uma ampla experiência prática.

Não importa se você pretende preencher as vagas de SOC por meio de recrutamento externo ou promoção interna, é um desafio encontrar profissionais para integrar a equipe que já venham "prontos" com todas as habilidades desejadas. É necessário treinamento constante, não só para preencher as lacunas entre os conjuntos de habilidades atuais e os necessários, mas também para capacitar os membros da equipe a lidar com tecnologias de segurança que mudam continuamente e um ambiente de ameaças que está sempre evoluindo.

Resposta a incidentes, perícia digital e análise de malware são competências indispensáveis.

RESPOSTA A INCIDENTES E PERÍCIA DIGITAL

- Responder a incidentes de maneira oportuna e precisa
- Analisar evidências (imagens de disco rígido, despejos de memória, rastreamento da atividade de rede) e reconstruir o histórico e a lógica dos incidentes
- Descobrir as supostas origens do ataque e outros sistemas que podem ter sido comprometidos (se possível)
- Entender a causa principal do incidente para impedir que outro incidente parecido aconteça

ANÁLISE DE MALWARE

- Entender a amostra do software suspeito e suas capacidades
- Definir se de fato se trata de um malware
- Determinar o impacto em potencial da amostra nos sistemas comprometidos dentro da organização
- Elaborar um plano de recuperação abrangente com base no comportamento do malware

A Kaspersky Lab oferece:
Serviços de treinamento em segurança cibernética

Há mais de 17 anos, a experiência em segurança cibernética da Kaspersky Lab, que inclui detecção de ameaças, pesquisa de malware, engenharia reversa e perícia digital, tem evoluído e avançado continuamente. Nossos especialistas sabem qual é a melhor maneira de lidar com as ameaças impostas pelas 325.000 amostras de malware que encontramos todos os dias e como divulgar esse conhecimento e a experiência prática para as organizações que se veem diante dos novos perigos da realidade cibernética contemporânea.

Nosso Programa de Treinamento em Segurança foi elaborado e desenvolvido pelas autoridades de segurança que ajudaram a montar os laboratórios de antivírus da Kaspersky e que hoje inspiram e orientam a próxima geração de especialistas do mundo todo.

Os cursos incluem tanto aulas teóricas quanto 'laboratórios' práticos. Depois de concluir cada curso, os alunos são convidados a comprovar seus conhecimentos fazendo uma avaliação.

Os cursos são apropriados para profissionais do setor de TI que possuem habilidades gerais ou avançadas de programação e de administração de sistemas. Todos os cursos estão disponíveis no formato de sala de aula no local do cliente ou em um dos escritórios locais ou regionais da Kaspersky Lab, conforme o caso.

DESCRIÇÃO DO PROGRAMA

TÓPICOS	DURAÇÃO	HABILIDADES ADQUIRIDAS
PERÍCIA DIGITAL		
• Introdução à perícia digital • Resposta em tempo real e aquisição de evidências • Estruturas internas do Registro do Windows • Análise de artefatos do Windows • Perícia em navegadores • Análise de e-mails	5 dias	• Montar um laboratório de perícia digital • Coletar evidências digitais e trabalhar com elas corretamente • Reconstruir um incidente e usar carimbos de data/hora • Encontrar vestígios de invasão com base em artefatos do Windows • Encontrar e analisar o histórico do navegador e de e-mail • Aplicar ferramentas e técnicas de perícia digital com segurança
ANÁLISE DE MALWARE E ENGENHARIA REVERSA		
• Objetivos e técnicas de análise de malware e engenharia reversa • Estruturas internas do Windows, arquivos executáveis, assembler x86 • Técnicas básicas de análise estática (extração de strings, análise de importação, visão geral de pontos de entrada PE, descompactação automática, etc.) • Técnicas básicas de análise dinâmica (depuração, ferramentas de monitoramento, interceptação de tráfego, etc.) • Análise de arquivos do .NET, Visual Basic, Win64 • Técnicas de análise de scripts e não PE (arquivos em lote; AutoIt; Python; JScript; JavaScript; VBS)	5 dias	• Montar um ambiente seguro para a análise de malware: implantar uma área restrita e todas as ferramentas necessárias • Entender os princípios da execução de programas no Windows • Descompactar, depurar e analisar um objeto malicioso, identificar suas funções • Detectar sites maliciosos por meio da análise de scripts de malware • Realizar a análise expressa de malware

TÓPICOS	DURAÇÃO	HABILIDADES ADQUIRIDAS
PERÍCIA DIGITAL AVANÇADA		
• Perícia detalhada no Windows • Recuperação de dados • Perícia em rede e na nuvem • Perícia na memória • Análise do desenrolar do incidente • Prática de perícia em ataques direcionados reais	5 dias	• Realizar uma análise minuciosa do sistema de arquivos • Recuperar arquivos excluídos • Analisar o tráfego de rede • Descobrir atividades mal-intencionadas usando despejos • Reconstruir o desenrolar dos incidentes
ANÁLISE DE MALWARE E ENGENHARIA REVERSA		
• Técnicas avançadas de análise estática (analisando o código shell estaticamente, analisando o cabeçalho PE, TEB, PEB, carregando funções por meio de diferentes algoritmos de hash) • Técnicas avançadas de análise dinâmica (estrutura PE, descompactação manual e avançada, descompactação de empacotadores maliciosos que armazenam o executável inteiro em formato criptografado) • Engenharia reversa de APTs (abordar um cenário de ataques de APTs, começando pelo e-mail de phishing e aprofundando o máximo possível) • Análise de protocolos (analisar o protocolo de comunicação C2 criptografada, como descriptografar o tráfego) • Análise de rootkits e bootkits (depurando o setor de inicialização usando Ida e VMWare, depurando o kernel usando duas máquinas virtuais, analisando amostras de rootkits)	5 dias	• Ser capaz de seguir as práticas recomendadas de engenharia reversa e, ao mesmo tempo, reconhecer truques antiengenharia reversa (obscurecimento, antidepuração) • Aplicar a análise avançada de malware para analisar rootkits/bootkits detalhadamente • Analisar exploits, código shell incorporado nos diferentes tipos de arquivos e malware não baseado no Windows
RESPOSTA A INCIDENTES		
• Introdução à resposta a incidentes • Detecção e análise primária • Análise digital • Criação de regras de detecção (YARA, Snort, Bro)	5 dias	• Diferenciar APTs de outras ameaças • Entender as diferentes técnicas utilizadas pelos invasores e a anatomia de um ataque direcionado • Aplicar métodos específicos de monitoramento e detecção • Seguir o fluxo de trabalho de resposta a incidentes • Reconstruir a cronologia e a lógica do incidente • Criar regras de detecção e relatórios

As ferramentas mudam com o tempo, mas os conceitos básicos e os métodos de trabalho permanecem consistentes. Os participantes vão receber não apenas um conjunto de ferramentas e instruções, mas um entendimento dos princípios e funcionalidades fundamentais. Todas as tarefas práticas são baseadas em casos reais, sempre que possível, sem violar a confidencialidade dos dados dos clientes.

INTELIGÊNCIA DE AMEAÇAS E BUSCA POR AMEAÇAS

Tradicionalmente, o SOC foi criado para oferecer:

- Gerenciamento dos dispositivos de segurança, manutenção do perímetro e tecnologias de segurança preventiva, como IPS/IDS, firewalls, proxies etc.
- Monitoramento de eventos de segurança através de um sistema de gerenciamento de informações e eventos de segurança (SIEM, Security Information and Event Management).
- Perícia e neutralização de incidentes.
- Conformidade interna ou normativa (por exemplo, PCI-DSS).

Muitas organizações agora estão se organizando para ter maior visibilidade das ameaças estabelecendo seus próprios

SOCs. No entanto, algumas organizações que já têm um SOC consideram que ainda enfrentam muitos dos mesmos problemas.

Existem inúmeros motivos para isso:

- Priorização inadequada, o que significa que as ameaças reais ficam perdidas entre milhares de alertas de segurança insignificantes recebidos e analisados a cada dia.
- A recuperação de incidentes sem um entendimento adequado de táticas, técnicas e procedimentos (TTPs, Tactics, Techniques and Procedures) dos agentes de ameaça associados, fazendo com que ataques avançados sejam negligenciados.
- Falsos negativos devido à falta de dados de ameaças correspondentes
- Uma abordagem reativa a incidentes, em vez de 'caçar' proativamente as ameaças que passam desapercebidas, mas que estão ativas na organização.
- Falta de uma visão geral estratégica do cenário de ameaças atual ou falta de conhecimento dos ataques em empresas semelhantes e das medidas corretivas disponíveis.

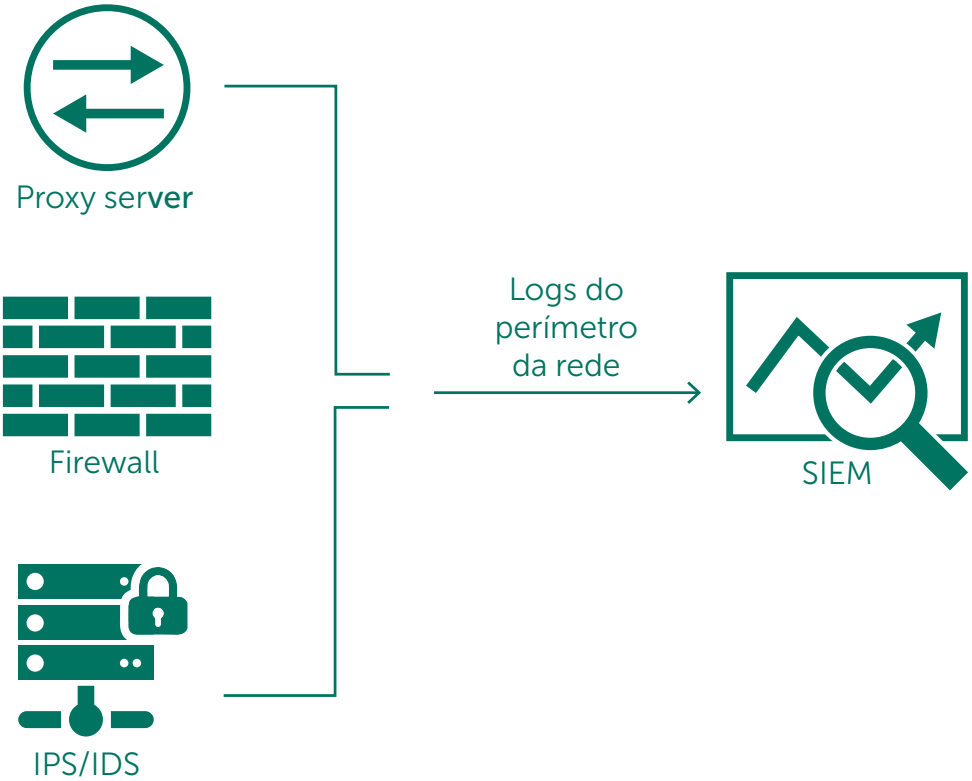


Figura 2:
Um SOC convencional

• Problema para atrair investimentos internos adequados em tecnologias de segurança específicas, devido a dificuldades para comunicar aos executivos do conselho que não são técnicos os riscos para os processos de negócio associados com violações de segurança.

A Gartner define inteligência de ameaças da seguinte forma:
"Conhecimento baseado em evidências, o que inclui contexto, mecanismos, indicadores, implicações e recomendações úteis sobre uma ameaça já existente ou emergente ou risco aos ativos, que pode ser usado para a tomada de decisões sobre a resposta a tal ameaça ou risco."

Gartner, How Gartner Defines Threat Intelligence, fevereiro de 2016

Com base nessas considerações, os líderes de segurança estariam bem assessorados para seguir uma abordagem de SOC orientada por informações. Para o SOC ser eficiente, deve sempre acomodar novas tecnologias e controles alinhados com as mudanças gerais no ambiente de ameaças constantes.

As ferramentas mudam com o tempo, mas os conceitos básicos e os métodos de trabalho permanecem consistentes. Os participantes vão receber não apenas um conjunto de ferramentas e instruções, mas um entendimento dos princípios e funcionalidades fundamentais. Todas as tarefas práticas são baseadas em casos reais, sempre que possível, sem violar a confidencialidade dos dados dos clientes.

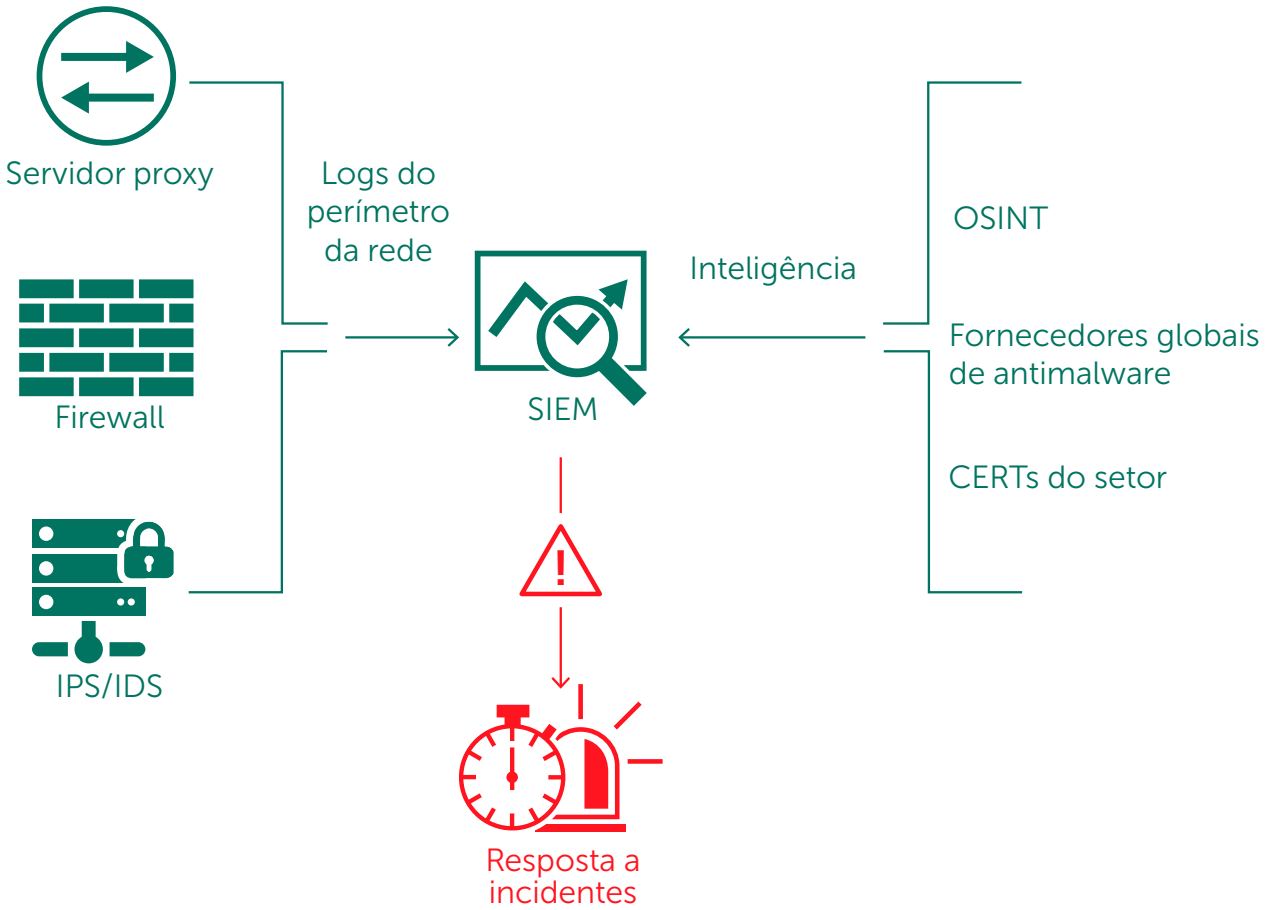


Figura 3:
O SOC orientado por informações

As fontes de informações devem ser escolhidas com cautela. Há uma correlação direta entre a qualidade das informações utilizadas e a efetividade das decisões tomadas com base nesses dados. Se você depende de informações irrelevantes, imprecisas ou não linhadas com os objetivos do seu setor ou negócio ou se as informações sobre ameaças não são recebidas prontamente, a qualidade do processo de tomada de decisões da sua organização pode ser seriamente comprometida.

Dados brutos sem contexto não vão conferir a relevância necessária para as equipes de SOC serem totalmente eficazes. Por exemplo, saber que um determinado URL é malicioso é muito diferente de também saber que ele é usado para hospedar um exploit ou um tipo específico de malware. Essa porção a mais de informações diz para seus especialistas em segurança o que eles devem procurar quando forem examinar a máquina infectada.

O que procurar em fontes externas de Inteligência de Ameaças:

- Informações de alcance global, que oferecem maior visibilidade do ataque
- Um provedor com experiência comprovada em identificar novos indicadores de ameaças com antecedência
- Inteligência rica em contexto e que permite tomar medidas de imediato
- Formatos de entrega e mecanismos que permitem uma integração fácil com controles de segurança já existentes

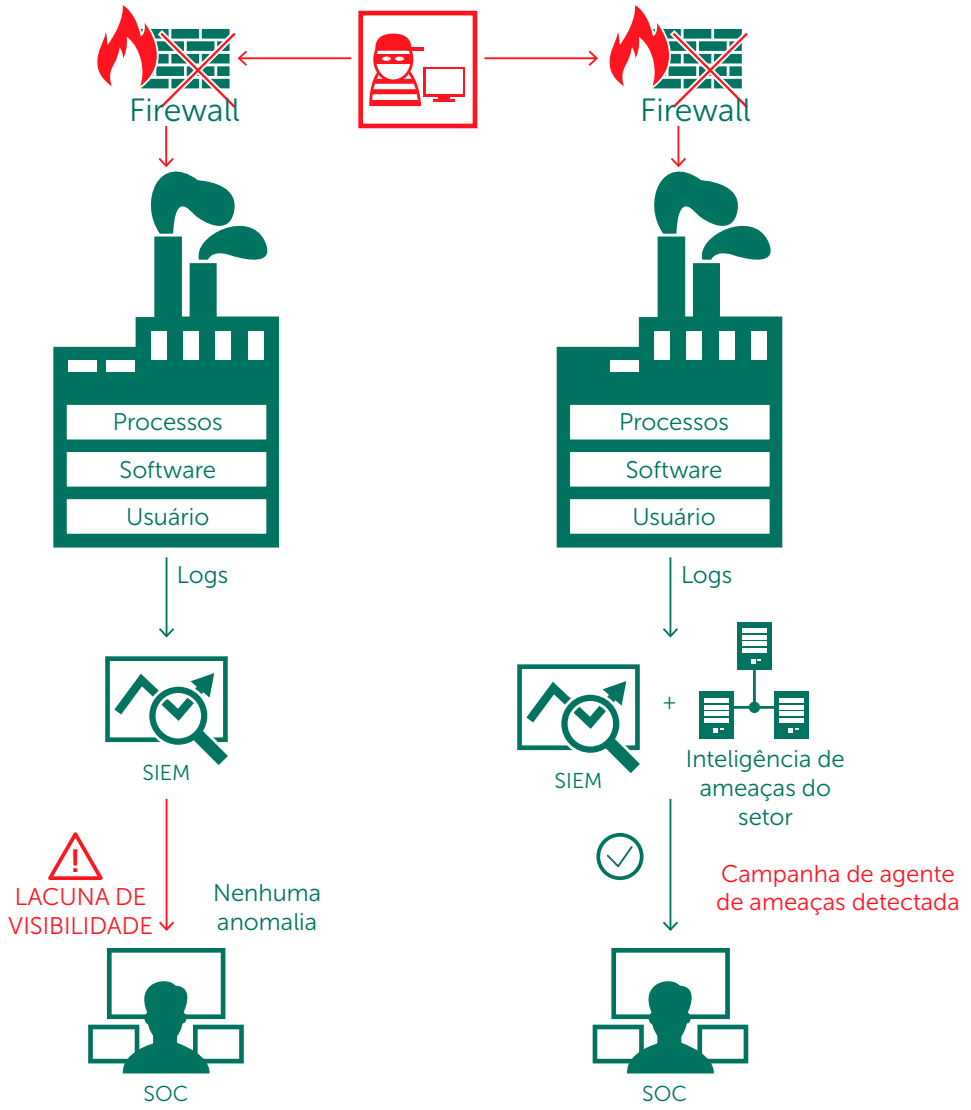


Figura 4:
Modelo de inteligência de ameaças

A busca por ameaças também é um elemento importante nas operações diárias do SOC. Esse não é um conceito novo. A detecção de ameaças desconhecidas e avançadas depende dos esforços práticos e diligentes dos analistas de segurança e não de regras automatizadas ou mecanismos de detecção baseados em assinatura.

Esse processo envolve agrupar e aplicar diferentes técnicas (como análise estática, aprendizado de máquina e visualização) a todos os dados disponíveis obtidos de endpoints, redes, controles de segurança implementados, sistemas de autenticação etc. O objetivo é confirmar uma hipótese relativa à possível ameaça. As tecnologias de busca de ameaças que o analista pode empregar incluem aquelas já mencionadas — soluções SIEM, OSINT, plataformas de inteligência de ameaças e outras fontes de dados.

O analista que busca ameaças vai consultar os indicadores de comprometimento (IOCs, Indicators of Compromise) obtidos externamente e aplicar ferramentas especializadas para procurar esses artefatos (na forma de endereços IP, hashes de arquivo, URLs etc.) nos hosts da organização. Quando for descoberto um sinal claro de comprometimento da segurança, poderão ser iniciados os procedimentos de resposta a incidentes.

Fazer buscas em volumes imensos de dados para identificar artefatos que não foram detectados por medidas automatizadas é uma tarefa para profissionais experientes e altamente qualificados.

A Kaspersky Lab oferece:
Feeds de Dados de Inteligência de Ameaças

A Kaspersky Lab oferece Feeds de Dados de Inteligência de Ameaças que são atualizados continuamente, para informar a sua equipe de SOC sobre os riscos e as implicações associados a ameaças virtuais, ajudando você a atenuar as ameaças de uma forma mais eficiente e se defender contra ataques antes mesmo de eles acontecerem.

DESCRIÇÃO DO PROGRAMA

Feeds de reputação de IP — um conjunto de endereços IP com contexto que abrange hosts suspeitos e maliciosos.
URLs maliciosos — um conjunto de URLs que abrange links e sites maliciosos. Registros mascarados e não mascarados estão disponíveis.
URLs de phishing — um conjunto de URLs identificados pela Kaspersky Lab como sendo sites de phishing. Registros mascarados e não mascarados estão disponíveis.
URLS de C&C de botnets — um conjunto de URLs de servidores C&C (comando e controle) de botnets e objetos maliciosos suspeitos.
Feeds de dados de lista branca — um conjunto de hashes de arquivo que fornecem a soluções e serviços de terceiros um conhecimento sistemático de software legítimo.
Feeds de hashes maliciosos — abrangendo os malwares mais perigosos, predominantes e emergentes.
Feeds de hashes maliciosos em dispositivos móveis — um conjunto de hashes de arquivo para detectar objetos maliciosos que infectam plataformas móveis.
Feeds de cavalo de Troia P-SMS — um conjunto de hashes de cavalo de Troia com o contexto correspondente para detectar cavalos de Troia SMS cobrando taxas premium dos usuários de dispositivos móveis e permitindo que um invasor roube, apague e responda mensagens SMS.
URLs de C&C de botnets móveis — um conjunto de URLs com contexto que abrange servidores C&C de botnets móveis.

DESTAQUES DO SERVIÇO

- Os Feeds de Dados são gerados automaticamente em tempo real, com base em descobertas no mundo inteiro (a Kaspersky Security Network proporciona visibilidade de uma porcentagem significativa de todo o tráfego da internet, cobrindo dezenas de milhões de usuários finais em mais de 200 países), oferecendo altas taxas de detecção e precisão.
- Todos os registros em cada Feed de Dados são enriquecidos com contexto prático (nomes das ameaças, carimbos de data e hora, localização geográfica, endereços IP resolvidos de recursos web infectados, hashes, popularidade etc.). Os dados contextuais ajudam a entender a 'situação como um todo', confirmando e permitindo o amplo uso desses dados. Quando no contexto, os dados podem ser usados mais prontamente para responder as perguntas quem, o que, onde e quando, que ajudam a identificar seus adversários, para que você possa tomar decisões em tempo hábil e tomar as medidas que vão proteger a sua organização.
- Formatos de disseminação simples (JSON, CSV, OpenIoC, STIX) via HTTPS ou mecanismos de entrega ad-hoc possibilitam a fácil integração dos feeds a soluções de segurança.
- A inteligência de ameaças é gerada e monitorada por uma infraestrutura altamente tolerante a falhas, garantindo a disponibilidade contínua e um desempenho consistente.
- Integração pronta para uso com HP ArcSight, IBM QRadar, Splunk e muito mais.

Kaspersky Threat Lookup

O Kaspersky Threat Lookup entrega todo o conhecimento necessário adquirido pela Kaspersky Lab sobre ataques virtuais e seus relacionamentos, reunindo tudo em um serviço Web avançado. O objetivo é fornecer às suas equipes de SOC o máximo de dados possível, impedindo os ataques virtuais antes que eles afetem a organização. A plataforma recupera as informações detalhadas mais recentes sobre ameaças, incluindo URLs, domínios, endereços IP, hashes de arquivo, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS etc. O resultado é a visibilidade global de ameaças novas e emergentes, ajudando a proteger sua organização e auxiliando na resposta a incidentes.

DESTAQUES DO SERVIÇO

- Informações confiáveis: Um atributo importante do Kaspersky Threat Lookup é a confiabilidade dos nossos dados de inteligência de ameaças, enriquecidos com contexto prático. Os produtos da Kaspersky Lab são líderes de mercado em testes de antimalware1, demonstrando a qualidade inigualável da nossa inteligência de ameaças ao oferecer as mais altas taxas de detecção, com falsos positivos próximos de zero.
- Altos níveis de cobertura em tempo real: As informações sobre ameaças são geradas automaticamente em tempo real, com base em descobertas no mundo inteiro e com o respaldo da Kaspersky Security Network.
- Busca de ameaças: seja proativo na prevenção, detecção e resposta a ataques para minimizar o impacto e a frequência deles. Rastreie e elimine os ataques ativamente tão logo quanto possível. Quanto antes você detectar uma ameaça, menor será o estrago causado, mais rápido ocorrerão os reparos e mais cedo a rede voltará a funcionar normalmente.
- Dados ricos: a inteligência de ameaças do Kaspersky Threat Lookup abrange uma imensa gama de tipos de dados, inclusive hashes, URLs, IPs, whois, pDNS, GeoIP, atributos de arquivos, dados estatísticos e comportamentais, cadeias de download, carimbos de data/hora, entre outros. Com esses dados, você pode pesquisar o cenário diverso de ameaças de segurança que tem enfrentado.
- Disponibilidade contínua: a inteligência de ameaças é gerada e monitorada por uma infraestrutura altamente tolerante a falhas, garantindo a disponibilidade contínua e um desempenho consistente.
- Revisão periódica por especialistas em segurança: centenas de especialistas, inclusive analistas de segurança de todas as partes do mundo, especialistas em segurança da nossa GReAT Team conhecidos no mundo inteiro e equipes de P&D de ponta, tudo contribui para gerar informações valiosas sobre ameaças reais.

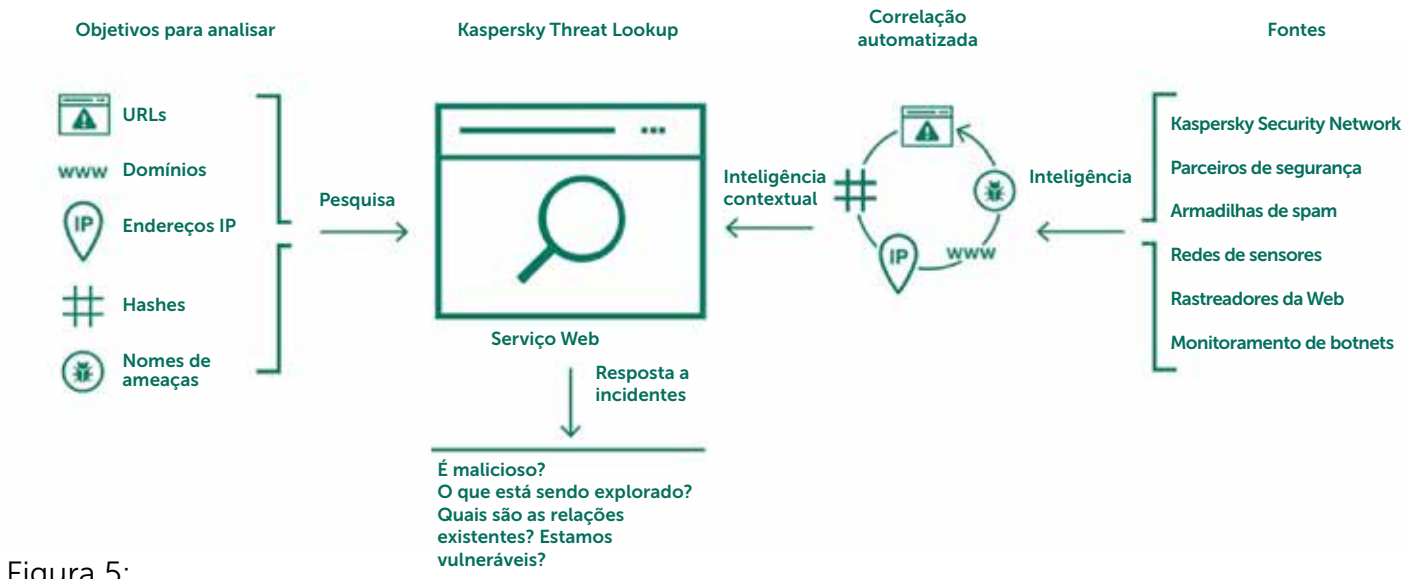
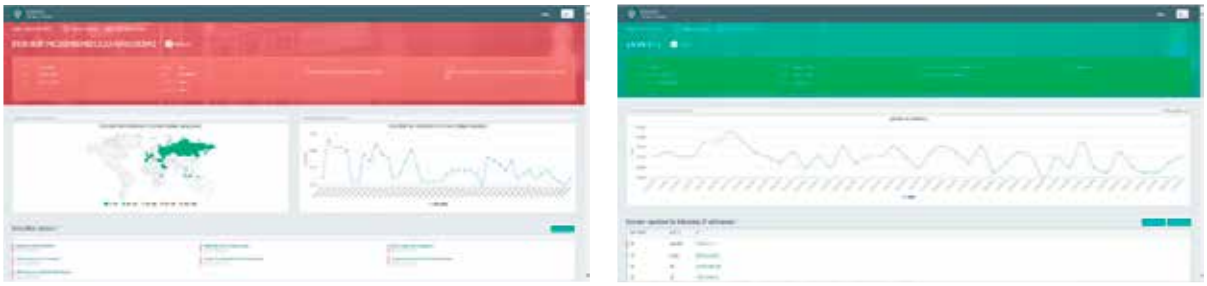


Figura 5:
Kaspersky Threat Lookup

1 http://www.kaspersky.com/top3

- Análise da área restrita: Detecte ameaças desconhecidas executando objetos suspeitos em um ambiente seguro e analise todo o escopo do comportamento da ameaça e os artefatos por meio de relatórios fáceis de interpretar.
- Ampla gama de formatos de exportação: Exporte IOCs ou contexto prático para formatos de compartilhamento legíveis por máquina amplamente usados e mais organizados, como STIX, OpenIOC, JSON, Yara, Snort ou até mesmo CSV, e aproveite todas as vantagens da inteligência de ameaças, automatize o fluxo de trabalho de operações ou faça a integração com controles de segurança como SIEMs.
- Interface Web ou API RESTful fáceis de usar: Use o serviço no modo manual através de uma interface web (via navegador) ou acesse por uma API RESTful simples, conforme a sua preferência.



Relatórios de inteligência de APTs

Nem todas as descobertas de ameaças persistentes avançadas são relatadas de imediato, e muitas nunca chegam ao conhecimento do público. Seja o primeiro a conhecer as nossas pesquisas mais recentes com o nosso exclusivo relatório detalhado de inteligência prática sobre APTs.

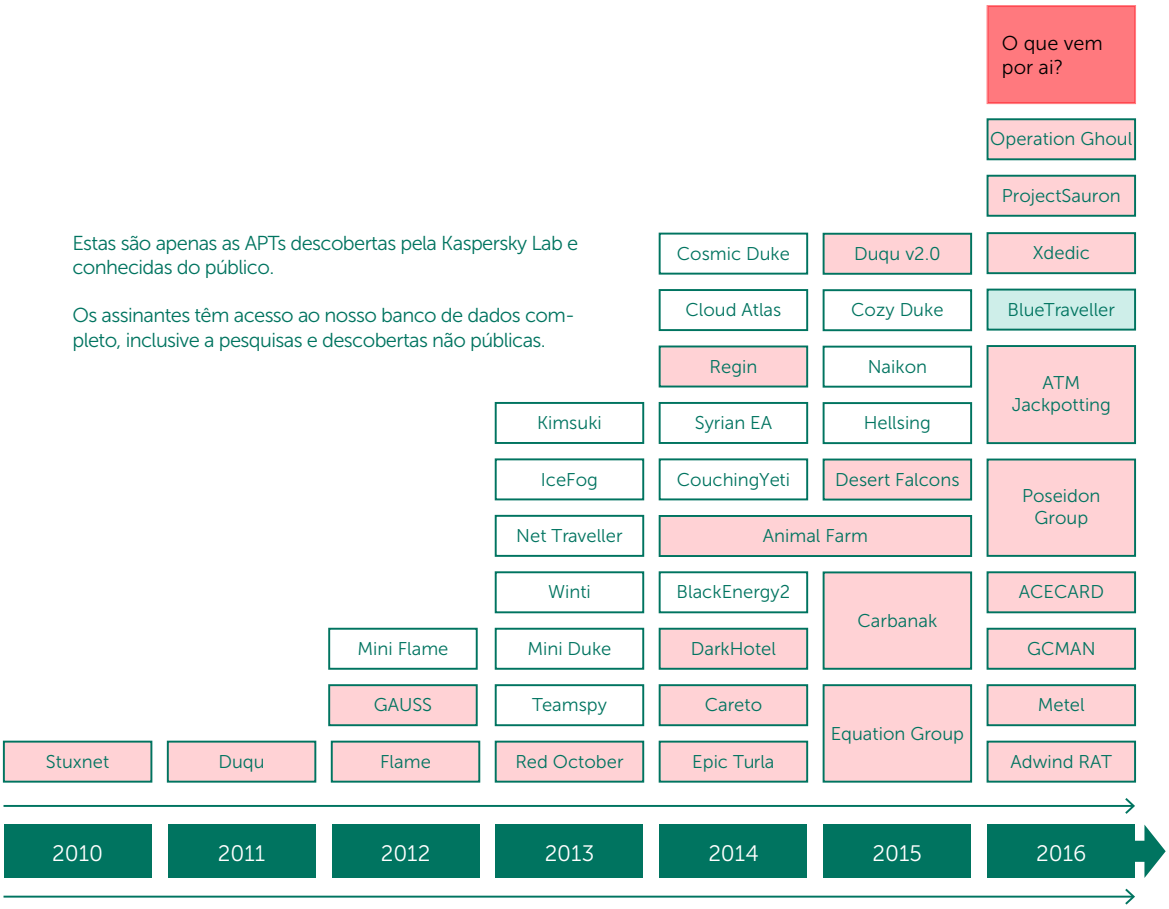


Figura 6:
APTs descobertas pela Kaspersky Lab

Como assinante do serviço de Relatórios de Inteligência de APTs da Kaspersky, você tem acesso contínuo e exclusivo às nossas investigações e descobertas, o que inclui dados técnicos na íntegra fornecidos em diversos formatos, sobre cada APT revelada, até mesmo de todas aquelas ameaças que nunca serão tornadas públicas. Os nossos especialistas, que são os mais gabaritados e bem-sucedidos caçadores de APT do setor, também vão alertar você imediatamente se detectarem quaisquer mudanças nas táticas de grupos que praticam crimes virtuais e terrorismo virtual. Além disso, você terá acesso ao banco de dados completo de relatórios de APT da Kaspersky Lab, um componente de pesquisa e análise muito poderoso da sua armadura de segurança corporativa.

DESTAQUES DO SERVIÇO

- Acesso exclusivo a descrições técnicas de ameaças inovadoras durante o processo de investigação, antes da divulgação ao público.
- Informações sobre APTs não públicas. Nem todas as ameaças ostensivas estão sujeitas a notificação pública. Algumas, devido às vítimas afetadas, à confidencialidade dos dados, à natureza do processo de correção de vulnerabilidades ou à atividade de aplicação das leis associadas, nunca são tornadas públicas. Mas todas são informadas aos nossos clientes.
- Dados técnicos complementares detalhados, amostras e ferramentas, inclusive uma ampla lista de IOCs, disponíveis no formato openIOC, e acesso às nossas Regras Yara.
- Monitoramento contínuo de campanhas de APT. Acesso a informações práticas durante a investigação (dados sobre distribuição de APTs, IOCs, infraestrutura de C&C).
- Análise retrospectiva – durante o período da sua assinatura, você tem acesso a todos os relatórios já emitidos.

Do ponto de vista prático, os indicadores de comprometimento são a parte mais prática do relatório para os especialistas de SOC. Essas informações estruturadas são fornecidas para uso posterior com ferramentas automatizadas específicas que ajudam a verificar se há sinais de infecção na sua infraestrutura.

Todos os relatórios são entregues através do Portal de Inteligência de APTs, como na ilustração a seguir.

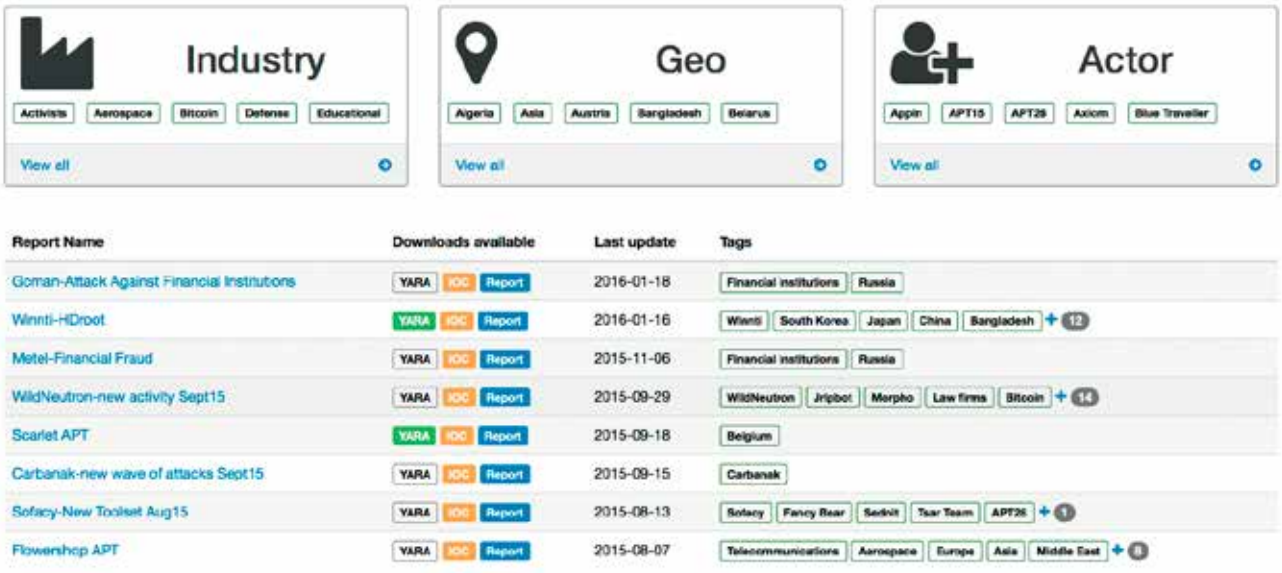


Figura 7:
Portal de Inteligência de APTs

Relatórios de ameaças personalizados

Relatórios de ameaças específicos para o cliente

Qual é a melhor maneira de montar um ataque contra a sua organização? Quais rotas e que informações estão disponíveis para um invasor que tem você como alvo específico? Já foi armado um ataque ou você está prestes a se tornar vítima de uma ameaça?

Os relatórios de ameaças específicos para o cliente da Kaspersky respondem essas perguntas e outras mais, enquanto os nossos especialistas compõem um quadro abrangente do seu status atual de ataques, identificando pontos fracos oportunos para a exploração e revelando evidências de ataques passados, atuais e planejados.

De posse dessas informações exclusivas, você pode concentrar sua estratégia de defesa nas áreas apontadas como alvos principais dos criminosos virtuais, agindo rapidamente e com precisão para repelir invasores e minimizar o risco de um ataque bem-sucedido.

Desenvolvidos usando inteligência de fontes abertas (OSINT, Open Source Intelligence), a análise profunda dos bancos de dados e especialistas em sistemas da Kaspersky Lab e o nosso conhecimento sobre redes clandestinas de criminosos virtuais, esses relatórios abrangem as seguintes áreas:

- Identificação de vetores de ameaça: identificação e análise do status de componentes críticos da rede disponíveis externamente, como ATMs, sistemas de vigilância por vídeo e outros que usam tecnologias móveis, perfis de funcionários em redes sociais e contas de e-mail pessoais, que são possíveis alvos de ataque.
- Análise e rastreamento de malware e ataques virtuais: identificação, monitoramento e análise de quaisquer amostras de malware ativo ou inativo direcionado para a sua organização, qualquer atividade de botnet anterior ou atual e qualquer atividade suspeita na rede.
- Ataques a terceiros: evidência de ameaças e atividade de botnet direcionadas especificamente para os seus clientes, parceiros e assinantes, cujos sistemas infectados poderiam ser usados para atacar você.
- Vazamento de informações: por meio de monitoramento discreto de fóruns e comunidades on-line clandestinos, descobrimos se há hackers discutindo planos de ataque que têm você como alvo ou, por exemplo, se um funcionário inescrupuloso está vendendo informações.
- Status de ataque atual: os ataques de APT podem continuar ocultos por muitos anos. Se detectarmos um ataque atual que esteja afetando a sua infraestrutura, damos orientação sobre como neutralizá-lo com eficiência.

INÍCIO RÁPIDO – FÁCIL DE USAR – NENHUM RECURSO NECESSÁRIO

Uma vez estabelecidos os parâmetros (dos relatórios específicos para o cliente) e os formatos de dados preferenciais, não é necessária nenhuma infraestrutura a mais para começar a usar esse serviço da Kaspersky Lab.

Os Relatórios de Inteligência de Ameaças da Kaspersky não afetam a integridade e a disponibilidade de recursos, inclusive dos recursos de rede.

Relatórios de ameaças específicos de país

A segurança cibernética de um país abrange a proteção de todas as suas instituições e organizações mais importantes. Ameaças persistentes avançadas (APTs, Advanced Persistent Threats) contra autoridades governamentais podem afetar a segurança nacional; possíveis ataques virtuais contra os setores de fabricação, transportes, telecomunicações, bancário e outros essenciais podem levar a danos consideráveis para o estado, como perdas financeiras, acidentes de produção, bloqueio de comunicações por rede e o descontentamento da população.

Tendo uma visão geral da superfície de ataque atual e das tendências em ataques por malware e invasões de hackers que visam o seu país, você pode concentrar a estratégia de defesa nas áreas apontadas como sendo os alvos principais dos criminosos virtuais, agindo rápido e com precisão para repelir os invasores e minimizar o risco de ataques bem-sucedidos.

Criados usando abordagens que variam desde OSINT à análise profunda de bancos de dados e sistemas por especialistas da Kaspersky Lab e o nosso conhecimento sobre redes clandestinas de criminosos virtuais, os relatórios de ameaças específicos de país abrangem áreas como:

- **Identificação de vetores de ameaça:** identificação e status de recursos de TI essenciais do país disponíveis externamente, como aplicativos governamentais vulneráveis, equipamentos usados em telecomunicações, componentes de sistemas de controle industrial (como SCADA, PLCs etc.), ATMs etc.
- **Análise e rastreamento de malware e de ataques virtuais:** identificação e análise de campanhas de APT, amostras de malware ativo ou inativo, atividade de botnet anterior ou atual e outras ameaças eminentes direcionadas para o seu país, com base em dados disponíveis nos nossos recursos de monitoramento internos exclusivos.
- **Vazamentos de informações:** por meio do monitoramento de fóruns e comunidades on-line clandestinas, descobrimos se há hackers discutindo planos de ataque com determinadas organizações em mente. Também revelamos contas comprometidas, que poderiam representar riscos para instituições e organizações atingidas (por exemplo, contas que pertencem a funcionários de órgãos governamentais disponíveis na violação de Ashley Madison, que poderiam ser usadas para chantagem).

O serviço de relatórios de inteligência de ameaças da Kaspersky não afeta a integridade e a disponibilidade dos recursos de rede que estão sendo inspecionados. O serviço tem como base métodos de reconhecimento de rede não invasivos e a análise das informações disponíveis em fontes abertas e recursos de acesso limitado.

Quando o serviço for concluído, você receberá um relatório contendo a descrição de ameaças eminentes relativas a diferentes setores e instituições do estado, além de outras informações sobre resultados de análises técnicas detalhadas. Os relatórios são entregues via e-mail criptografado.

O serviço pode ser fornecido como projeto de uso único ou periodicamente por assinatura (por trimestre, por exemplo).

Relatórios de ameaças específicos de país

O serviço Proteção Gerenciada da Kaspersky oferece o Kaspersky Security for Business e a Kaspersky Anti Targeted Attack Platform, uma combinação exclusiva de medidas técnicas avançadas para detectar e impedir ataques direcionados. O serviço inclui monitoramento ininterrupto por especialistas da Kaspersky Lab e análise contínua de dados de ameaças virtuais (inteligência de ataques virtuais), garantindo a detecção em tempo real de campanhas conhecidas e novas de espionagem cibernética e de crimes virtuais visando sistemas de informações críticos.

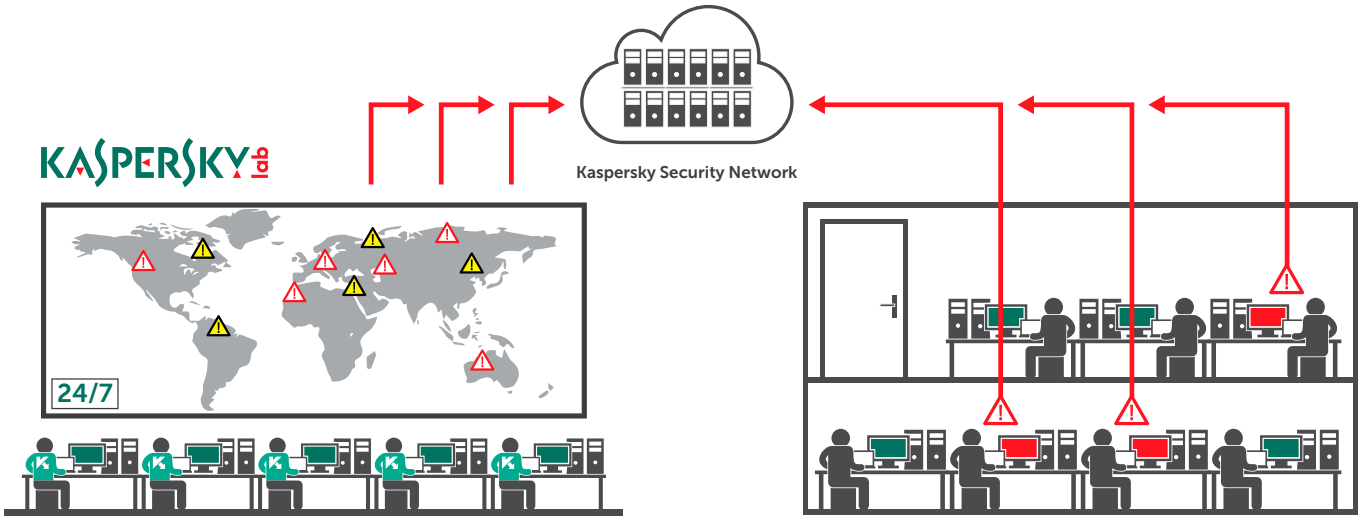


Figura 8:
Proteção Gerenciada da Kaspersky

DESTAQUES DO SERVIÇO

- Proteção de alto nível contra ataques direcionados e malware, com suporte 24 horas por dia, 7 dias por semana, dos analistas da Kaspersky Lab.
- Informações sobre os invasores, suas motivações, os métodos e ferramentas usados por eles e os danos em potencial que eles poderiam causar, possibilitando o desenvolvimento de uma estratégia de proteção eficiente e bem embasada.
- A detecção de ataques não relacionados a malware, ataques envolvendo ferramentas desconhecidas e ataques que exploram vulnerabilidades de dia zero.
- Análise retrospectiva de incidentes e busca de ameaças.
- Redução dos custos gerais de segurança e, ao mesmo tempo, aumento da qualidade da proteção. Trata-se de um serviço altamente profissional oferecido pela sua líder mundial em análise de ataques virtuais e inclui análise dos métodos e tecnologias utilizados por agentes de ameaça. Obter esse nível de informação por meio de um serviço externo é muito mais econômico do que empregar especialistas com áreas de atuação mais restritas.
- Abordagem integrada — através da nossa ampla linha de soluções integradas Kaspersky Security for Business, a Kaspersky Lab oferece todas as tecnologias e os serviços necessários para implementar um ciclo de proteção completo contra ataques direcionados: Preparação — Detecção — Investigação — Análise de dados — Proteção automatizada.

BENEFÍCIOS DO SERVIÇO

- Detecta incidentes rapidamente.
- Coleta informações em quantidade suficiente para permitir a classificação (como falso positivo ou detecção correta).
- Identifica o quão comum são os artefatos coletados, determinando o grau de singularidade do ataque.
- Inicia o processo de responder a um incidente de segurança de informações.
- Inicia quaisquer atualizações necessárias de bancos de dados de antivírus, para bloquear a disseminação de ameaças.

Mais sobre as fontes de inteligência de ameaças da Kaspersky

A inteligência de ameaças é agregada a partir de uma fusão de fontes heterogêneas e altamente confiáveis, como a Kaspersky Security Network (KSN) e os nossos rastreadores da Web, nosso serviço de Monitoramento de Botnet (monitoramento de botnets e seus alvos e atividades, 24 horas por dia, 7 dias por semana, 365 dias por ano), armadilhas de spam, equipes de pesquisa, parceiros e outros dados históricos sobre objetos maliciosos coletados pela Kaspersky Lab durante quase duas décadas. Depois, em tempo real, todos os dados agregados são cuidadosamente inspecionados e refinados através de diversas técnicas de pré-processamento, como critérios estatísticos, sistemas especializados da Kaspersky Lab (áreas restritas, mecanismos de heurística, ferramentas de análise de similaridade, perfis comportamentais etc.), validação por analistas e verificação de lista branca.

Tendo pessoal devidamente capacitado e treinado e uma inteligência de ameaças adquirida de fontes confiáveis e implementada nos controles de segurança existentes, chegou o momento de pensar na sua resposta a incidentes.

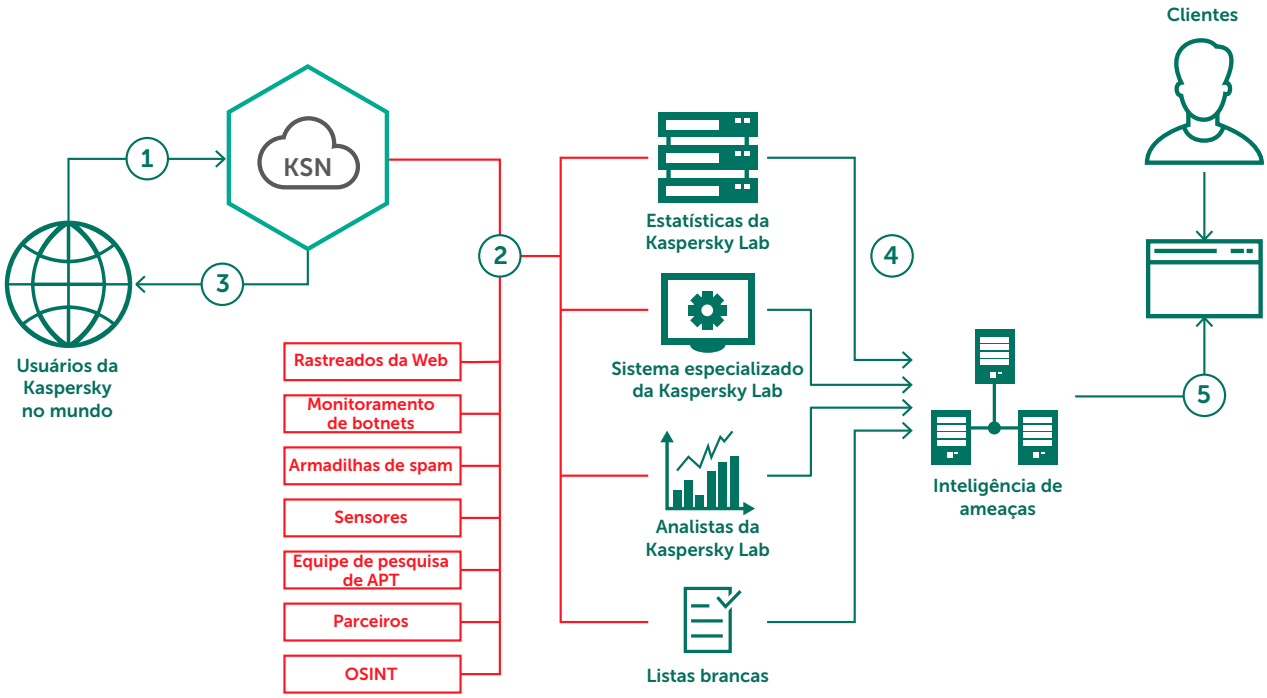


Figura 9:
Fontes de inteligência de ameaças da Kaspersky Lab

ESTRUTURA DE RESPOSTA A INCIDENTES

Perícia e resposta a incidentes requer a alocação de recursos internos consideráveis sem aviso. Especialistas bem instruídos, com grande experiência prática no combate a ameaças virtuais, terão de agir rapidamente para identificar, isolar e bloquear a atividade mal-intencionada. Rapidez é essencial quando se quer minimizar as consequências e os custos da recuperação.

Dominar esse nível de conhecimento a curto prazo pode ser um desafio, mesmo para uma equipe de SOC já bem estabelecida – são poucas as organizações que possuem recursos internos suficientes disponíveis para interromper um ataque avançado. Além disso, há casos, como APTs ou ameaças complexas patrocinadas por algum país, em que a equipe de SOC não tem conhecimento especializado das abordagens e táticas específicas utilizadas pelos agentes de APT envolvidos.

Em casos como esses, pode ser mais econômico e produtivo trabalhar junto com uma consultoria ou um prestador de serviços de resposta a incidentes, que vai estar preparado aplicar uma resposta rápida e plenamente embasada.

Uma estrutura abrangente de resposta a incidentes deve incluir o seguinte:

- **Identificação de incidentes**
  Análise inicial de incidentes e isolamento dos sistemas infectados
- **Aquisição de evidências**
  Dependendo do tipo de incidente, será preciso inspecionar diferentes fontes para obter as evidências necessárias
- **Análise pericial (se necessário)**
  Nessa fase, é possível formar um panorama detalhado do incidente
- **Análise de malware (se necessário)**
  Para entender as funcionalidades do malware
- **Plano de recuperação**
  Desenvolvimento de um plano para erradicar a causa básica do problema e todos os vestígios do código malicioso
- **Lições aprendidas**
  Análise e atualização dos controles de segurança existentes para evitar incidentes semelhantes

Figura 10:
Estrutura de resposta a incidentes

A Kaspersky Lab oferece:
Serviços de resposta a incidentes

O nosso serviço de resposta a incidentes é de altíssima qualidade e abrange todo o ciclo de investigação do incidente, desde a aquisição de evidências no local até a identificação de outros indicadores de comprometimento, a preparação de um plano de recuperação e a completa eliminação da ameaça à sua organização. As investigações da Kaspersky Lab são realizadas por investigadores e analistas de detecção de invasões virtuais muito experientes. Toda a relevância da nossa expertise global em perícia digital e análise de malware pode ser empregada na resolução do seu incidente de segurança.

Estes são os objetivos que devem ser atingidos durante a execução do serviço:

- Identificar recursos comprometidos.
- Isolar a ameaça.
- Impedir que o ataque se espalhe.
- Encontrar e coletar evidências.
- Analisar as evidências e reconstruir a cronologia e a lógica do incidente.
- Analisar o malware utilizado no ataque (caso seja encontrado algum).
- Descobrir a origem do ataque e outros sistemas potencialmente comprometidos (se possível).
- Com o auxílio de ferramentas, realizar varreduras em toda a sua infraestrutura de TI para descobrir possíveis sinais de comprometimento.
- Analisar conexões de saída entre sua rede e recursos externos para detectar qualquer coisa suspeita (como possíveis servidores de C&C).
- Eliminar a ameaça.
- Recomendar outras medidas de recuperação que você possa tomar.

Dependendo de você ter ou não sua própria equipe de resposta a incidentes, você pode pedir para os nossos especialistas realizarem todo o ciclo de investigação, para simplesmente identificar e isolar as máquinas comprometidas e impedir a disseminação da ameaça ou para conduzir a análise de malware ou a perícia digital.

ANÁLISE DE MALWARE

Com a análise de malware, é possível entender o comportamento e os objetivos dos arquivos de malware específicos direcionados para a sua organização. Os especialistas da Kaspersky Lab realizam uma análise minuciosa da amostra de malware fornecida por você, criando um relatório detalhado que inclui os seguintes dados:

- Propriedades da amostra: uma breve descrição da amostra e um veredito sobre a classificação do malware.
- Descrição detalhada do malware: uma análise detalhada das funções da amostra de malware, comportamento e objetivos da ameaça (incluindo IOCs), de modo que você tenha todas as informações necessárias para neutralizar as atividades.
- Cenário de recuperação: o relatório vai sugerir medidas para proteger totalmente a sua organização contra esse tipo de ameaça.

PERÍCIA DIGITAL

A perícia digital pode incluir análise de malware, mencionada acima, caso algum malware tenha sido descoberto durante a investigação. Os especialistas da Kaspersky Lab reúnem as evidências para entender exatamente o que está acontecendo, o que inclui o uso de imagens de HDD, despejos de memória e vestígios de rede. O resultado é o esclarecimento detalhado do incidente. Como cliente, você inicia o processo coletando evidências e apresentando um resumo do incidente. Os especialistas da Kaspersky Lab analisam os sintomas do incidente, identificam o binário do malware (se existir) e realizam a análise de malware para fornecer um relatório detalhado que inclui as medidas de recuperação.

PERÍCIA DIGITAL

Os serviços de resposta a incidentes da Kaspersky Lab estão disponíveis:

- Por assinatura
- Em resposta a um único incidente

As duas opções são baseadas no tempo gasto pelos nossos especialistas para resolver o incidente. Isso é negociado com o cliente antes da assinatura do contrato. O cliente poderá incluir o número de horas de trabalho que ele considera necessárias ou seguir as recomendações dos nossos especialistas de acordo com cada caso específico.

POR QUE ESCOLHER A KASPERSKY LAB?

Porque nós temos:

- Parcerias com autoridades legais do mundo todo, como Interpol e CERTs
- Ferramentas na nuvem que monitoram milhões de ameaças virtuais no mundo inteiro em tempo real
- Equipes globais que analisam e tomam conhecimento de ameaças da internet de todos os tipos

Porque somos:

- A maior empresa de software de segurança independente do mundo, dedicada a inteligência de ameaças e liderança em tecnologia
- Líder incontestável em testes de detecção de malware mais independentes do que qualquer outro fornecedor
- Considerados Líder pela Gartner, Forrester e IDC

Sobre a Kaspersky Lab

A Kaspersky Lab é o maior fornecedor privado de soluções de proteção de endpoints do mundo. A empresa está classificada entre os quatro principais fornecedores de soluções de segurança para usuários de endpoints do mundo. Durante os seus mais de 18 anos de história, a Kaspersky Lab continua sendo inovadora em segurança de TI e fornece soluções de segurança digital eficientes para consumidores, pequenas e médias empresas e grandes corporações. Com sua empresa matriz registrada no Reino Unido, a Kaspersky Lab opera em quase 200 países e territórios ao redor do globo, fornecendo proteção para mais de 350 milhões de usuários em todo o mundo.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab