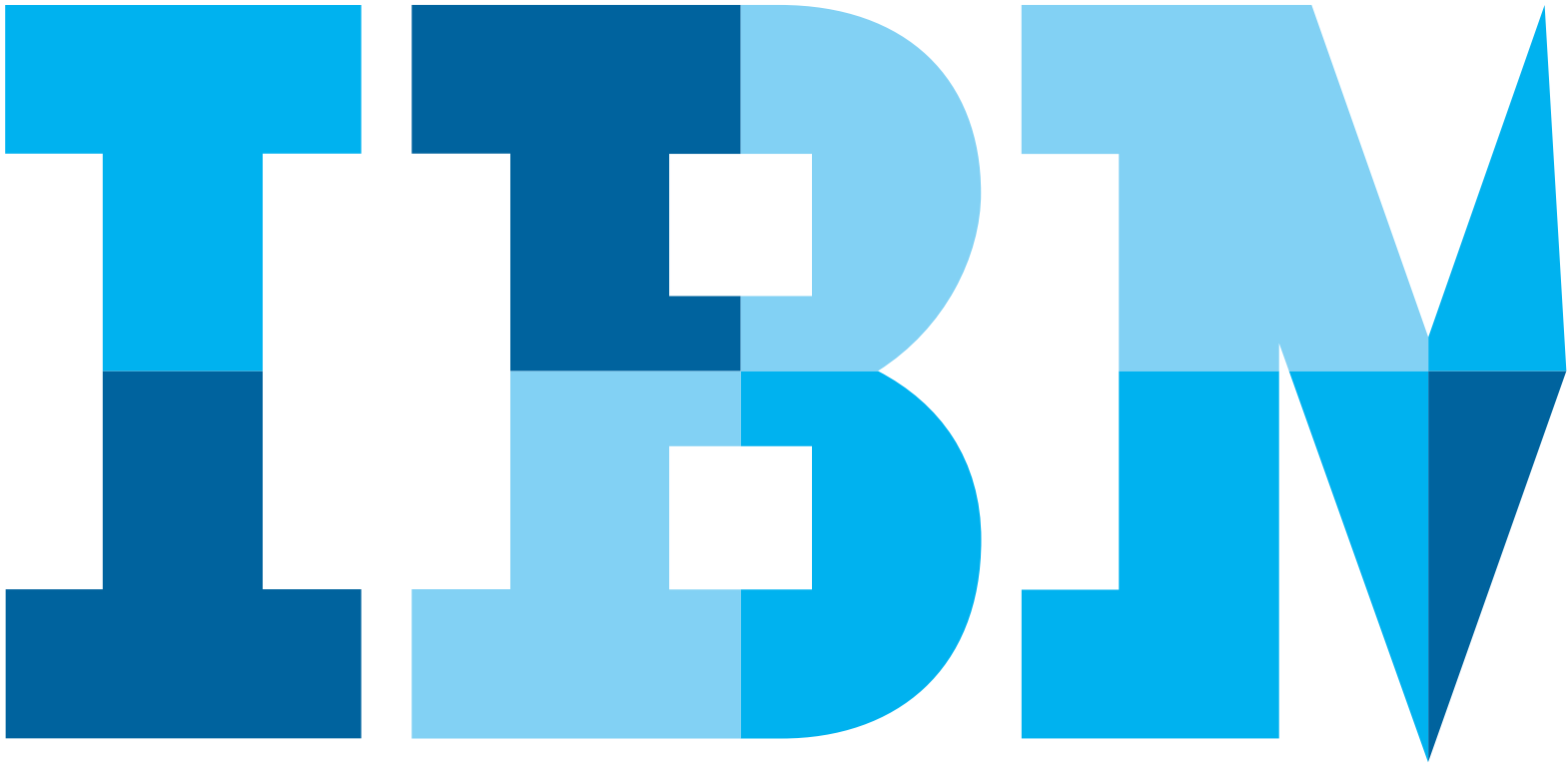
Serviços Gerenciados de Segurança

Ajudando a reforçar a segurança da sua empresa por meio de melhores práticas de entrega de serviço



IBM

1

Visão Geral

Um breve resumo dos Serviços de Segurança IBMServiços de Segurança IBM e dos desafios de negócios abordados

2

Implemen-tação

Uma análise da solução IBM, incluindo seus recursos, componentes técnicos e o custo

3

Entrega de Serviço

Como a IBM gerenciará seus ativos de segurança, monitorará seu ambiente, analisará dados de eventos e lidará com incidentes de segurança

4

Suporte e Relatórios

Nosso portal do cliente, gerenciamento de problemas e as ferramentas de consulta e relatório que podem ajudá-lo a gerenciar seu ambiente de segurança

5

Próximos Passos

Passos que você pode dar e recursos que pode explorar para aprender mais sobre os Serviços de Segurança IBM

1. Visão Geral

A necessidade de proteção

Empresas de todos os portes travam uma batalha contínua para se defender de invasores online que podem atacar a qualquer momento. Seja na forma de um vírus, ataque de negação de serviço ou acesso não autorizado ao banco de dados, ataques à segurança bem-sucedidos causam estragos ao interromper operações de negócios, reduzir a produtividade da mão de obra, danificar a infraestrutura e prejudicar a reputação e o valor da marca. As responsabilidades associadas ao gerenciamento inadequado da segurança estão se tornando mais graves; vão desde os recursos necessários para solucionar a violação, tempo de inatividade caro e possível perda de negócios até multas por falta de conformidade regulamentar.

Embora as ameaças de segurança de TI continuem evoluindo, as organizações têm de lidar com orçamentos reduzidos, prioridades concorrentes e ambientes mais complexos. Os departamentos de segurança de TI de hoje precisam oferecer um nível mais alto de proteção por um custo significativamente reduzido.

Entretanto, as organizações que gerenciam sua própria segurança de informações muitas vezes não têm os recursos internos necessários para proteger sistemas online 24 horas por dia, sete dias por semana. Práticas de segurança avançadas exigem profissionais altamente qualificados, cujo recrutamento, contratação e retenção podem ser caros. Além disso, a implementação e o gerenciamento de soluções de segurança podem desviar recursos de TI de outras iniciativas essenciais, incluindo a prevenção do próximo ataque.

Serviços de Segurança IBMServiços de Segurança IBM

Os Serviços de Segurança IBMServiços de Segurança IBM para equipamentos nas instalações do cliente (ver Tabela 1) são concebidos para oferecer monitoramento e gerenciamento contínuos e quase em tempo real da tecnologia de segurança de vários fornecedores, ajudando você a proteger o valor dos seus investimentos existentes em segurança enquanto reduzem a complexidade e o custo das suas operações de segurança.

Esses serviços gerenciados podem ser usados individualmente ou em combinação para ajudar organizações a:

- Melhorar a postura de segurança e mitigar riscos para as operações de negócios

- Reduzir o custo do gerenciamento da segurança
- Simplificar o gerenciamento e reduzir a complexidade
- Abordar a escassez de qualificações essenciais
- Fornecer suporte ao gerenciamento de conformidade.

A IBM também oferece uma linha abrangente de serviços de segurança gerenciados hospedados, bem como uma solução para Proteção Gerenciada de Negação de Serviço Distribuída (DDoS). Ao combinar ofertas do portfólio completo de serviços gerenciados complementares da IBM, é possível aumentar suas economias de custo e sua inteligência de segurança. Isso acontece porque a infraestrutura de operações de segurança global da IBM foi

Gerenciamento de Firewall—monitoramento de firewall 24 horas por dia, sete dias por semana, encaminhamento, relatório de incidente e assistência à correção.	
• Check Point NGX / R71 e posterior	• Cisco • Juniper Netscreen
Gerenciamento Unificado de Ameaças—gerenciamento 24 horas por dia, sete dias por semana com suporte para recursos de produtos UTM abrangentes (firewall, IPS/ IDS, antivírus, antispam, filtragem na web, SSL VPN).	
• IBM Proventia® Network Multi- Function Security • Check Point UTM-1, Edge e IP Appliance	• Cisco ASA, ISR • Juniper SSG, ISG + IDP, SRX • Palo Alto Networks • Fortinet FortiGate
Gerenciamento de Detecção e Prevenção de Intrusão—monitoramento de ameaças 24 horas por dia, sete dias por semana, encaminhamento, relatório de incidente e assistência à correção.	
• IBM Network Intrusion Prevention System • IBM Security Server Protection • Cisco IDS, IPS, IDP • Juniper IDP	• McAfee Intrushield, M Series IPS • SourceFire • Check Point IPS-1

Gerenciamento de Informações e Eventos de Segurança Gerenciado (SIEM)—Fornece monitoramento por especialistas 24 horas por dia, sete dias por semana e resposta para as ferramentas de SIEM do cliente.	
• IBM Q1 Labs® QRadar®	• HP ArcSight
Gateway da Web Seguro Gerenciado—Proteção contínua de transações essenciais baseadas na web.	
• BlueCoat SG (Proxy)	• BlueCoat AV (w/ SG)
Serviços de Proteção Gerenciados—Proteção 24 horas por dia, sete dias por semana, além de gerenciamento, monitoramento e encaminhamento por especialistas em tempo real para redes e terminais corporativos. **Serviços de Gerenciamento de Vulnerabilidades**—Varreduras de segurança contínuas que ajudam a identificar e priorizar vulnerabilidades encontradas em dispositivos de rede, sistemas operacionais, aplicativos da web e bancos de dados.	

Tabela 1. Os Serviços de Segurança IBMServiços de Segurança IBM (equipamentos nas instalações do cliente) e o suporte a dispositivos

concebida para integrar dados de diversos serviços de segurança gerenciados, ajudando você a unir silos de TI e tecnologias, além de obter uma visualização de ponta a ponta do seu cenário de segurança (ver Figura 1). O resultado final são mais informações, correlacionadas pela IBM quase em tempo real para análise profunda e resposta mais rápida a ameaças.

Recursos do serviço

Os Serviços de Segurança IBMServiços de Segurança IBM oferecem ferramentas, tecnologias e conhecimentos líderes no setor juntamente com um pacote flexível e escalável para cumprir uma ampla gama de requisitos. Não importa se você compra serviços gerenciados para um ou para vários tipos de dispositivos; sua solução de segurança incluirá:

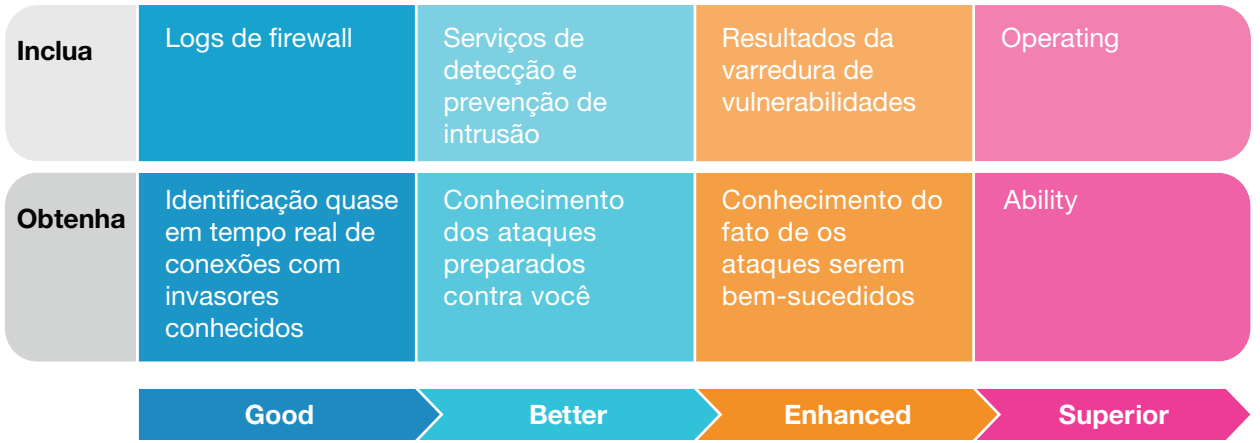


Figure 1. Combining IBM Managed Security Services offerings can help increase your analytic capabilities.

- O portal do cliente do Centro de Operações de Segurança Virtual (SOC Virtual) baseado na web que oferece um “console único” por meio do qual é possível gerenciar seu ambiente de segurança e seus serviços IBM
- Acesso a especialistas em segurança
- Upgrades e atualizações contínuos
- Relatórios padronizados e customizáveis
- Operações com a certificação SSAE 16 em todos os nossos Centros de Operações de Segurança (SOCs) de ponta, que são concebidos para alta disponibilidade
- Precificação com taxa fixa simplificada padronizada em nosso conjunto principal de serviços, com camadas de precificação que oferecem flexibilidade para selecionar os níveis de serviço mais adequados para seu ambiente de segurança
- Inteligência e relatórios de segurança da organização de pesquisa de segurança global IBM X-Force®.

Configuração flexível dos níveis de serviço

Com a IBM, você adquire a flexibilidade necessária para configurar seus serviços de segurança gerenciados a fim de cumprir seus requisitos de tempo de resposta, disponibilidade de dispositivo e custo. É possível escolher entre pacotes de serviço pré-configurados que simplificam o processo de compra ou você pode começar com o serviço de base e, depois, especificar as opções de nível de serviço por dispositivo, por local ou até mesmo com granularidade dispositivo por dispositivo. Por exemplo, por dispositivo, suas opções de configuração podem incluir:

- Retenção de dados do log (um, três, cinco ou sete anos)
- Tarifa única ou tarifa mensal para taxas de iniciação de serviço e configuração de dispositivo
- Análise e alerta automatizados ou monitoramento e alerta “visuais” por um Analista de Ameaças da IBM
- Tempos de resposta de alerta (níveis de serviço de 15, 30 ou 60 minutos)
- Tempos de resposta de Solicitação de Mudança de Política (níveis de serviço de 2, 4, 8, 12 ou 24 horas)
- Notificação de eventos de funcionamento de dispositivo (níveis de serviço de 15, 30 ou 60 minutos)
- Aplicativo de atualização de dispositivo (níveis de serviço de 24, 48 ou 72 horas)

- Disponibilidade de dispositivo, incluindo opções para gerenciamento de um dispositivo redundante “warm standby” e configurações de alta disponibilidade de dispositivos agrupados.

IBM X-Force Threat Analysis Service

O IBM X-Force Threat Analysis Service está incluído com todas as ofertas de Serviços de Segurança IBM e integrado no portal do cliente. Esse serviço de inteligência de segurança líder no setor ajuda você a gerenciar ameaças diárias de segurança proativamente, pois fornece uma avaliação de condições de ameaças online globais e análise detalhada adequada às suas necessidades.

O X-Force Threat Analysis Service consiste em uma mistura de inteligência de segurança confiável da organização de pesquisa e desenvolvimento IBM Security X-Force, dados de ameaças coletados a partir da rede internacional de centros de operações de segurança da IBM e mais de 30.000 sensores de rede, agentes e dispositivos gerenciados ou monitorados, assim como ameaças globais da Internet monitoradas 24 horas por dia, sete dias por semana pelo centro de operações de ameaças globais da IBM.

O nível de ameaça da Internet global é atualizado em tempo real pela equipe da X-Force e informado usando o sistema de classificação AlertCon™, um indicador concebido para medir o nível de ameaça a ativos online em um momento específico. Além do status atual do AlertCon, o X-Force Threat Analysis Service oferece informações customizadas sobre ameaças e notícias de segurança relevantes para suas plataformas, produtos e negócios. Informações detalhadas sobre os relatórios do X-Force Threat Analysis Service e a seção X-Force do portal SOC virtual estão disponíveis na Seção 4 deste guia.

2. Implementação

Ativação de serviços

A IBM utiliza um processo estruturado em cinco fases para ajudar a garantir a implementação tranquila dos seus serviços de segurança gerenciados (ver Figura 2). Como regra geral, as implementações são concluídas em um prazo de 30 a 60 dias—embora projetos pequenos possam levar apenas alguns dias, enquanto projetos muito grandes podem ser implementados em estágios durante um período de vários meses.

- **Início**. Seu Engenheiro de Implementação (DE) designado, que será seu ponto único de contato durante a implementação, revisará o pedido com você e estabelecerá contato com os vários membros da sua equipe. Seu DE trabalhará com sua equipe para determinar uma linha de tempo e avaliar o status dos seus sites.
- **Planejamento**. Durante essa fase, o DE trabalhará com sua equipe para planejar como os novos dispositivos de segurança serão colocados na sua rede; como a IBM gerenciará e monitorará seus dispositivos e dados de segurança por vários canais de comunicação criptografados; e agendar datas de instalação e ativação de serviço mais definitivas.
- **Preparação**. Conforme o caso, o DE providenciará a configuração dos novos dispositivos de segurança que você comprou ou forneceu à IBM, seja remotamente ou em um dos nossos centros de implementação. Seu DE também preparará a arquitetura de gerenciamento na IBM para seus dispositivos de segurança.
- **Integração**. Nessa fase, novos dispositivos de segurança são instalados e sua funcionalidade correta é testada; é estabelecida uma conectividade entre seus dispositivos existentes e o Centro de Operações de Segurança (SOC). Depois que um teste mostra que o SOC é capaz de monitorar e gerenciar seus dispositivos de segurança, seu DE fará a transição do gerenciamento de dispositivo para o SOC e demonstrará o portal do cliente do SOC Virtual para sua equipe.

- Conclusão. Seu DE finalizará os itens finais de implementação e promoverá ou providenciará uma chamada introdutória com a equipe do SOC que prestará seus serviços de segurança 24 horas por dia, sete dias por semana. A partir desse momento, seu contato principal será com o SOC, com o DE disponível para você para questões pendentes finais e perguntas sobre a transição.

Estabelecimento de políticas de linha de base

Exceto se for solicitado, a IBM implementa novos dispositivos e agentes com uma política de linha de base padrão desenvolvida pelo Centro de Operações de Segurança da IBM. As políticas de linha de base da IBM geralmente refletem as recomendações de política padrão dos respectivos fornecedores de produto. Isso inclui quais assinaturas estão ativadas e quais respostas estão configuradas para cada assinatura. No entanto, com base em tendências e ameaças emergentes detectadas por analistas de segurança da IBM, as políticas de linha de base também podem incluir desvios em relação às recomendações dos fornecedores.

Processo de implementação e integração de Managed Security Services

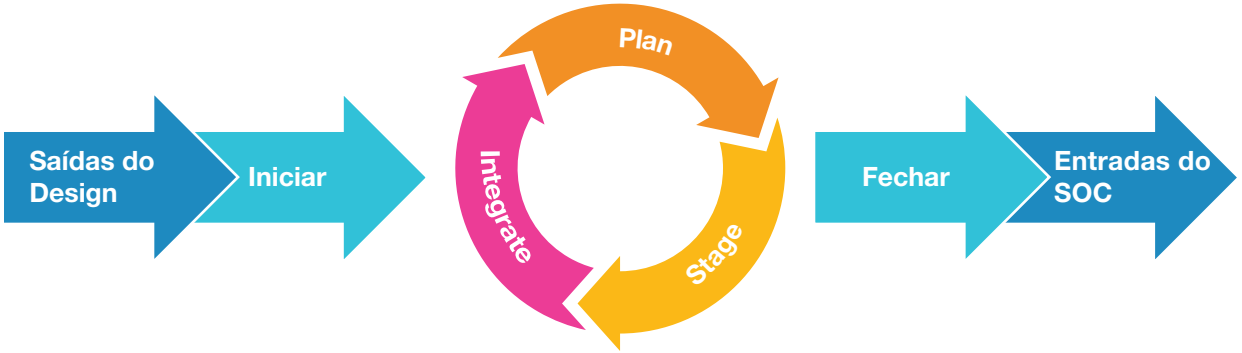


Figura 2. O processo estabelecido da IBM para implementar e integrar seus dispositivos em nossa infraestrutura de gerenciamento foi concebido para assegurar a implementação tranquila dos seus serviços de segurança gerenciados.

No caso de dispositivos e agentes existentes, a IBM recomenda a substituição das políticas existentes por políticas de linha de base da IBM quando você migrar para o SOC para gerenciamento. Isso pode ajudar a eliminar configurações incorretas anteriores que criaram buracos na segurança e substituir ajustes desatualizados ou ineficazes por uma linha de base consistente em todos os dispositivos gerenciados.

No caso de clientes que têm diferentes dispositivos e agentes do mesmo modelo, versão ou sistema operacional, a IBM compartilha políticas sempre que possível. As políticas compartilhadas proporcionam consistência na cobertura de segurança, permitem a implementação mais rápida de novas assinaturas e outras mudanças de política e ajudam a facilitar auditorias eficientes.

Funções e responsabilidades: Operações de segurança da IBM

Para gerenciar a infraestrutura de segurança de cada cliente de maneira efetiva e eficiente, além de assegurar que as qualificações adequadas sejam aproveitadas nas operações, a IBM dividiu a equipe de SOC em três grupos principais:

- Os Analistas de Ameaças trabalham 24 horas por dia, sete dias por semana; tratam diretamente de eventos acionáveis que são filtrados para o console de operações do SOC Virtual. Esses analistas monitoram diferentes origens de dados, respondem a alertas e investigam e encaminham incidentes de segurança.
- A Equipe de Gerenciamento de Dispositivo trabalha 24 horas por dia, sete dias por semana; é responsável pelo gerenciamento do funcionamento e da disponibilidade dos dispositivos.
- Esses especialistas em segurança trabalham com os clientes para resolver problemas em dispositivos, realizar manutenção e upgrades, implementar mudanças de política e fornecer suporte técnico.
- A Equipe de Garantia e Padrões de Serviço monitora processos para controle de qualidade, realiza treinamentos e executa gerenciamento de projetos de planejamento e operacionais.

Resposta a um incidente de segurança: quem está encarregado?

Apesar de a IBM ser responsável por monitorar seu ambiente de segurança suportado, gerenciar o funcionamento dos seus dispositivos e analisar eventos e alertas, sua Equipe de Resposta a Incidentes de Segurança de Computador (CSIRT) é responsável por verificar e agir em relação a incidentes reais—encaminhados pelo SOC ou sua própria equipe de TI.

Sua Equipe de Resposta a Incidentes deve ser orientada pelo Plano de Resposta a Incidentes de Segurança de Computador (CSIRP) da sua organização, que oferece um mapa para lidar com um ataque de segurança. Ele deve definir as funções e responsabilidades de todos os respondentes, estabelecer autoridade para tomar as principais decisões e definir os fluxos de comunicação e procedimentos de notificação.

Durante sua resposta, é essencial que sua equipe e a equipe do SOC permaneçam se comunicando. De sua parte, o SOC continuará prestando assistência e oferecendo recomendações, conforme o caso, até que o incidente seja resolvido e encerrado.

Funções e responsabilidades: equipe de segurança de TI do cliente

Para ajudar a assegurar seu sucesso no uso de Serviços de Segurança IBM, é fundamental que você designe profissionais para executar as seguintes responsabilidades de segurança de modo efetivo. A forma como uma organização preenche essas funções depende de seu tamanho. No caso de organizações pequenas, uma única pessoa poderia, possivelmente, executar todas as responsabilidades. Em organizações grandes, diferentes indivíduos podem ser necessários para cumprir estas responsabilidades:

- Interagir com o serviço de segurança gerenciado por meio do portal do cliente para revisar status de dispositivo, chamados abertos, incidentes de segurança e informações sobre ameaças da X-Force
- Documentar redes, dispositivos, servidores e outros ativos do cliente
- Revisar as políticas dos dispositivos e iniciar solicitações de mudança
- Determinar quando encaminhamentos, dentro da organização do cliente e do SOC, são necessários
- Responder a encaminhamentos iniciados pelo SOC e coordenar recursos internos adequados.

3. Entrega de Serviço

Centro de Operações de Segurança

A rede global de Centros de Operações de Segurança (SOCs) interconectados da IBM funciona como o principal agente de entrega para todos os Managed Security Services. Cada SOC está localizado dentro de uma instalação experiente da IBM que fornece protocolos de segurança padrão do setor para segurança física e lógica. Os SOCs da IBM possuem certificações SSAE16 (Statement on Standards for Attestation Engagements, número 16) e funcionam de acordo com normas de governança de organizações como ISO e o Federal Financial Institutions

Examination Council (FFIEC), bem como as rigorosas normas de segurança de TI da própria IBM.

Uma arquitetura tecnológica comum e a rede integrada de serviços de segurança gerenciados permitem que todos os SOCs funcionem como uma única operação coesiva conhecida como Centro de Operações de Segurança Virtual (SOC Virtual); qualquer SOC é capaz de ver todos os dispositivos gerenciados e monitorados. Hardware e software padronizados, juntamente com políticas e procedimentos comuns, impingem o gerenciamento e o monitoramento uniformes de dispositivos do cliente, assim como SLAs e controle de mudanças gerenciados globalmente.

Com a estrutura do SOC Virtual, uma equipe completa de especialistas em segurança fica disponível 24 horas por dia durante os dias úteis, com uma equipe mais limitada em finais de semana e feriados (ver Figura 3). Além disso, cada SOC tem visibilidade dos outros. Por meio do uso de webcams, voz sobre IP e um painel digital para engenheiros do SOC, os engenheiros do SOC podem agir e sentir como se cada SOC estivesse logo ao lado, independentemente de a quantos milhares de quilômetros de distância eles podem estar realmente localizados.

A atividade do SOC global é organizada a partir de um centro de comando e controle centralizado localizado em Atlanta, Geórgia (EUA). Aqui, ocorrem balanceamento de carga de trabalho, failover de dispositivo gerenciado e correlação e análise de eventos. A instalação de Atlanta também funciona como Centro de

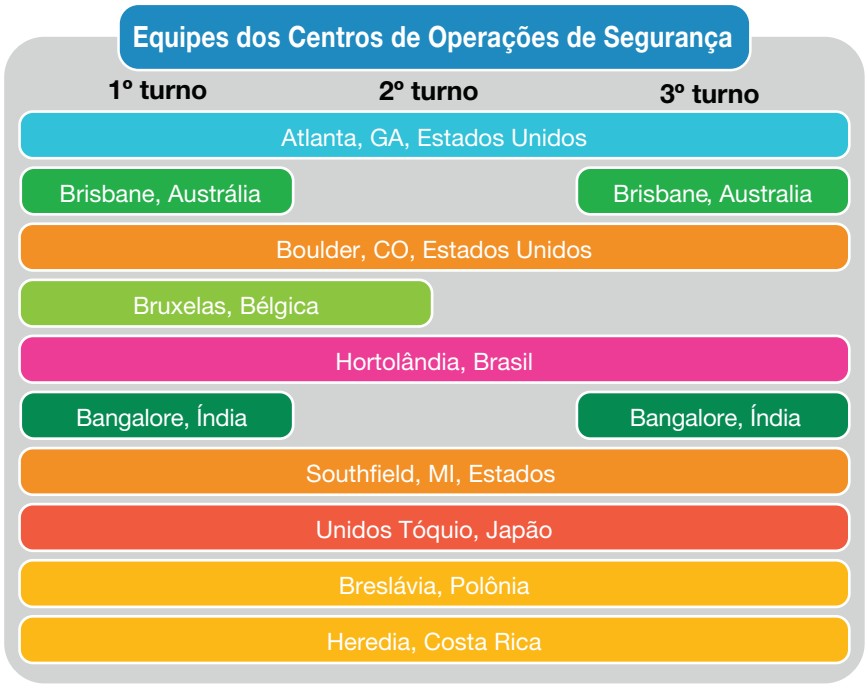


Figura 3. Centros de operações de segurança (SOCs) globalmente integrados e equipes em tempo integral possibilitam o gerenciamento e o monitoramento de segurança 24 horas por dia, sete dias por semana.

Operações de Ameaças Globais (GTOC) da IBM. Nele, informações sobre ameaças são correlacionadas, tendências globais são identificadas e sínteses diárias para as muitas agências do governo que recebem suporte da IBM—incluindo o Departamento de Segurança Interna dos Estados Unidos, o Information Technology Information Sharing and Analysis Center (IT-ISAC) e a Agência Federal de Investigação (FBI)—são realizadas por chamada de conferência todas as manhãs.

Gerenciamento de dispositivo

Um dos principais componentes dos Serviços de Segurança IBM é a capacidade de gerenciamento de dispositivo remoto, que permite que a equipe do SOC realize atividades diárias essenciais, tais como resolução de problemas, gerenciamento de configuração, gerenciamento de log, instalação de upgrades e monitoramento geral de dispositivo (ver Figura 4). Por meio do monitoramento remoto, o SOC é capaz de detectar falhas na conectividade ou outros problemas anormais que poderiam afetar negativamente sua segurança e operações de negócios.

Se um evento impossibilitar o gerenciamento de um dispositivo por uma conexão na banda, a IBM trabalhará com sua equipe designada para identificar as causas da indisponibilidade e determinar se a perda de conectividade representa um incidente maior que poderia afetar a segurança ou as operações. A IBM emite um chamado de problema e rastreia o problema até a resolução.

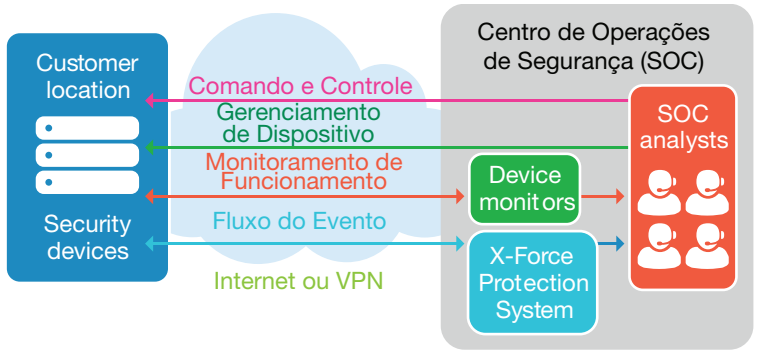


Figure 4. This high-level view of the Managed Security Services architecture shows the data flow between the managed devices at the customer location and the SOC.

Ajuste de política e mudanças de política

Geralmente, depois de duas a quatro semanas de operações em estado estável, seus dispositivos gerenciados terão produzido dados do evento suficientes para o ajuste de política. Seus analistas podem avaliar esses dados para identificar oportunidades para alinhar melhor as políticas de linha de base padrão estabelecidas pela IBM no início do serviço com seu tráfego de rede. Tal esforço pode ajudar a reduzir positivos falsos e a quantia de análise de dados necessária para monitorar sua rede, ajudando a focar a resposta a incidentes em eventos reais.

Não importa se foram solicitadas como resultado de decisões de ajuste iniciais, em função de mudanças no cenário de ameaças ou em resposta a eventos reais: mudanças de política para dispositivos gerenciados pela IBM são consideradas como solicitações padrão, com prazos de implementação determinados por níveis de serviço contratados. As solicitações de mudança de política—por exemplo, uma mudança de política de firewall ou uma mudança na assinatura de detecção de intrusão—são enviadas pelo portal do SOC Virtual como chamados e executadas por um engenheiro do SOC. O sistema de chamados ajuda você a monitorar suas mudanças de política ao longo do tempo e ajuda a garantir que sejam implementadas corretamente.

Atualizações e correções

Novo conteúdo de segurança e assinaturas, assim como aprimoramentos de produto, atualizações de firmware e correções de bugs, são liberados mensalmente, no mínimo, e com mais frequência, quando necessário, com base no ambiente de ameaças da Internet atual. Atualizações de emergência podem ser disponibilizadas no prazo de 24 horas após a descoberta de uma nova vulnerabilidade. Todas as atualizações e comunicações associadas são coordenadas com o cliente por meio do sistema de chamados no SOC Virtual.

Em geral, as atualizações de conteúdo de segurança contêm novas informações de assinatura e pequenas atualizações no dispositivo. Não incluem mudanças no sistema operacional do dispositivo ou em drivers de hardware; dessa forma, geralmente não afetam as redes monitoradas

nem exigem uma janela de manutenção. O SOC aplica essas atualizações de conteúdo automaticamente, a menos que os clientes especifiquem algo diferente. O processo de atualização começa

dentro de um número específico de horas após o registro de data e hora da liberação oficial do fornecedor do dispositivo, tal como informado no seu acordo de nível de serviço. No caso de produtos de segurança da IBM, há uma liberação mensal regular X-Press Update (XPU) imediatamente após a liberação de correção mensal da Microsoft. A IBM também libera XPUs de emergência conforme necessário para abordar explorações de dia zero e outros problemas urgentes de segurança.

Para atualizações de firmware, o SOC revisa cada liberação à medida que é anunciada pelo respectivo fornecedor para determinar a criticidade da atualização. Se a liberação de firmware abordar uma vulnerabilidade de segurança significativa no produto, o SOC cria um chamado com detalhes específicos e trabalha com você para agendar uma janela de manutenção para realizar a atualização. Se, em caso de investigação, o SOC considerar que uma atualização de firmware não é essencial, ela será tratada como opcional.

Monitoramento e análise de eventos

Os Serviços de Segurança da IBM são dedicados a fornecer aos clientes o nível mais elevado de serviços de proteção para ajudar a abordar vulnerabilidades e proteger de ameaças baseadas na Internet. A primeira linha de defesa é o X-Force Protection System (XPS), uma ferramenta exclusiva da IBM que manipula a coleta, arquivamento e análise de todos os logs e eventos monitorados pelo SOC (ver Figura 4).

Um evento de segurança é definido como a saída de um dispositivo ou aplicativo de segurança. Os exemplos de eventos de segurança incluem alertas de sensores de detecção/prevenção de intrusão (IDPS) ou logs de firewall. O mecanismo de correlação XPS utiliza análise estatística sofisticada e correlação baseada em regras para separar eventos reais de “ruído” nos dados provenientes desses dispositivos (ver Figura 5).

Os analistas altamente qualificados do SOC da IBM monitoram e avaliam continuamente os dados de eventos filtrados quase em tempo real para identificar incidentes de segurança. Esses analistas correlacionam em diferentes origens e tipos de dados, incluindo inteligência de segurança da X-Force e a postura de segurança do cliente. Como parte da triagem inicial de eventos, os analistas do SOC utilizam seu profundo conhecimento de vulnerabilidades e vetores de ataque para eliminar alarmes falsos rapidamente. Os analistas do SOC também são treinados para descobrir eventos que são mais difíceis de identificar, como incidentes de segurança "baixos e lentos", bem como ameaças persistentes avançadas.

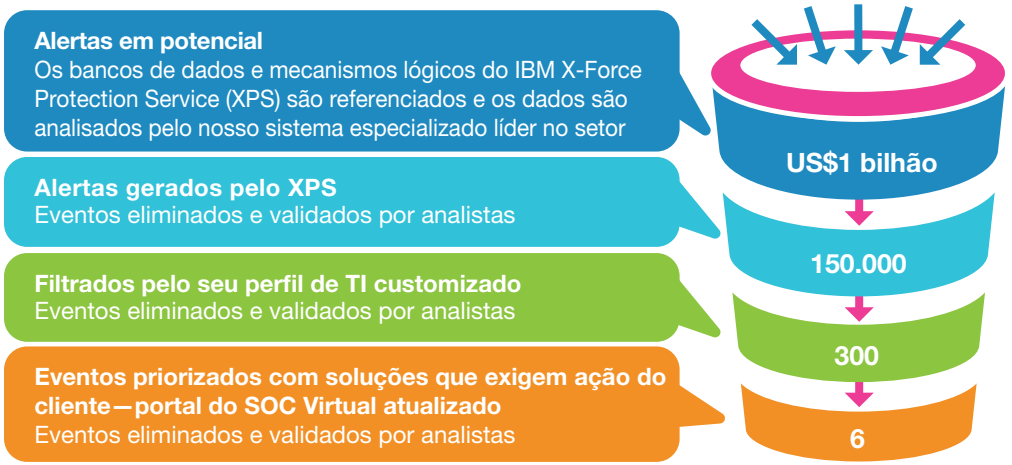


Figura 5. A IBM utiliza diferentes camadas de análise por sistemas especialistas e analistas qualificados para filtrar o "ruído" e priorizar eventos com base no seu ambiente.

Gerenciamento de incidente

Os eventos que não podem ser descartados imediatamente acionam uma revisão abrangente de dados de vulnerabilidade, incidentes de segurança do passado, diagramas de rede do cliente e correlação cruzada em tempo real de tendências de ataque globais. Os analistas do SOC utilizam uma metodologia em seis fases para investigar cuidadosamente atividades anômalas ou suspeitas.

Fase 1: Inteligência e análise de ataques

A inteligência da IBM X-Force fornece uma base para a triagem inicial de eventos. Utilizando informações sobre como as explorações funcionam, os analistas do SOC correlacionam padrões de atividades com a gravidade da assinatura para associar o comportamento com ataques conhecidos. Desse modo, o analista do SOC consegue determinar os riscos em potencial associados aos eventos.

Fase 2: Investigações de origem e destino

Essa investigação varia com base no fato de as máquinas de origem e destino serem internas ou externas à rede de um cliente.

No caso de máquinas internas, o SOC faz referência cruzada com relação a diagramas de rede monitorada, informações críticas do servidor e, quando estão disponíveis, dados da varredura de vulnerabilidades. No caso de máquinas externas, os analistas fazem referência cruzada com relação aos bloqueios de IP da lista de bloqueio da X-Force, invasores conhecidos e investigações e encaminhamentos do passado.

Fase 3: Classificação e priorização de incidentes

Nem todas as investigações de atividades suspeitas resultam na declaração de um incidente de segurança: a maioria dos eventos é classificada como “não acionável”. Esses eventos são acionados por tráfego malicioso no ambiente do cliente—por exemplo, a presença de tráfego de worm em massa em uma rede—mas as redes e servidores visados não são vulneráveis às explorações. A menos que um servidor do cliente esteja infectado e propagando um worm de forma ativa, não há necessidade de ação e o evento não é encaminhado.

Somente depois de um exame e de uma análise cuidadosos dos dados um evento é classificado como um incidente de segurança que exige ação, sendo priorizado de acordo com a gravidade da ameaça. A IBM utiliza as seguintes categorias de incidentes para ajudar a orientar as ações subsequentes:

- **Código malicioso**: Um vírus, worm, cavalo de Troia ou outra entidade baseada em código que infectou ou comprometeu um sistema interno com êxito e começou a propagar dentro de redes ou sistemas internos
- **Análises e varreduras**: Atividades de reconhecimento em uma rede destinadas a descobrir sistemas e facilitar o mapeamento da rede
- **Negação de serviços**: Um ataque que prejudica o uso de redes, sistemas ou aplicativos ao esgotar os recursos de conexão e largura da banda; os ataques de negação de serviço (DoS) e negação de dispositivo distribuída (DDoS) se encaixam nessa categoria
- **Acesso não autorizado**: Acesso lógico não autorizado a uma rede, sistema, aplicativo, dados ou outro recurso, incluindo comprometimentos de raiz, alterações não autorizadas em dados e desfigurações de websites
- **Uso inadequado**: Violações de políticas de uso aceitável, tais como aplicativos de compartilhamento de arquivos peer-to-peer e outros usos indevidos ou abusos de recursos
- **Análise de tendências**: Atividade anômala dentro de um fluxo de evento padrão para um dispositivo específico que exige uma revisão histórica de um fluxo de evento, o que normalmente não é realizado em tempo real.

Após a classificação, o analista do SOC prioriza o incidente correlacionando três fatores (ver Figura 6). Os incidentes de segurança são designados a um dos três níveis de prioridade:

- **Prioridade 1**: Incidentes nesse nível são eventos acionáveis de alto risco que têm o potencial de causar danos graves aos ambientes do cliente. Eventos de Prioridade 1 exigem que os clientes executem ações defensivas imediatas. Comprometimentos de sistema ou dados, infecções e propagação de worm, ataques maciços de negação de serviço (DOS) e incidentes semelhantes recebem esse nível de prioridade.

Figura 6. Os analistas do SOC priorizam incidentes com base em três critérios.

- **Prioridade 2**: É o nível mais baixo de incidentes acionáveis. Os incidentes de Prioridade 2 exigem que os clientes executem ações no prazo de 12 a 24 horas após a notificação pelo SOC. Incidentes como atividade de varredura local não autorizada e ataques direcionados a servidores ou estações de trabalho específicos recebem esse nível de prioridade.

- **Prioridade 3**: Os incidentes dessa categoria envolvem atividade em uma rede ou servidor que não é diretamente acionável. Varredura de descoberta e vulnerabilidade, scripts de coleta de informações e outras análises de reconhecimento recebem esse nível de prioridade.

Fase 4: Encaminhamento de incidentes
Depois que um incidente é identificado, classificado e priorizado, a IBM o encaminha à sua equipe de segurança autorizada para manipulação. Os níveis de serviço contratados determinam com que rapidez os incidentes de segurança serão encaminhados; as opções de nível de serviço são tempos de resposta de 15, 30 ou 60 minutos. Os clientes podem configurar preferências para métodos de notificação preferenciais—por exemplo, telefone, telefone celular, email ou pelo portal. Durante o encaminhamento de um incidente de segurança de Prioridade 1, a IBM tentará se comunicar com o contato do cliente designado até a notificação ocorrer com êxito ou até que todos os contatos de encaminhamento tenham sido esgotados.

Fase 5: Recomendações de contramedida
Após comunicar um contato autorizado durante o encaminhamento de um incidente de segurança de Prioridade 1, o analista do SOC recomendará ações adequadas para impedir ou conter o ataque.

As contramedidas disponíveis para o SOC e os clientes variam com base nos serviços e plataformas gerenciados pela IBM no site afetado. Uma lista de contramedidas e suas propriedades associadas está detalhada na Tabela 2.

Tipo de Contramedida	Ação Padrão da IBM	Exige Autorização	Plataformas
Bloqueio Reativo	Não	Sim	IBM IDS/ IPS
Eliminar	Não	Sim	Todos os IDS/ IPS de rede e host
Notificação ISP	Sim	Não	Todos
Mudança em política de firewall ou ACL	Não	Sim	IBM IDS/ IPS ou firewall gerenciado

Tabela 2. Os analistas do SOC trabalharão com você para determinar as ações que podem ser executadas para impedir ou conter um ataque.

Observação importante: ***A Equipe de Resposta a Incidentes do cliente é responsável por verificar e agir de acordo com incidentes encaminhados pelo SOC, em conformidade com o Plano de Resposta a Incidentes de Segurança de Computador (CSIRP) da organização. À medida que sua equipe executa o CSIRP, é essencial que você e a equipe do SOC IBM permaneçam se comunicando. De sua parte, o SOC continuará prestando assistência e oferecendo recomendações, conforme o caso. Caso sua organização não tenha um CSIRP consistente ou uma capacidade de resposta a emergências, a IBM oferece serviços de consultoria de segurança capazes de abordar suas necessidades específicas.***

Fase 6: Documentação

O estágio final do encaminhamento de qualquer incidente de segurança é a documentação. Todos os aspectos da atividade e do ataque são documentados dentro de um chamado e um relatório de incidente de segurança. Informações sobre o chamado e o relatório estão disponíveis para os clientes em tempo real pelo portal do cliente do SOC Virtual.

4. Suporte e Relatórios

Portal do cliente do SOC Virtual

O portal do cliente do SOC Virtual é um portal baseado na web que funciona como centro de comando centralizado para monitoramento e controle de dispositivos de segurança sob gerenciamento da IBM. Está disponível online 24 horas por dia, sete dias por semana, a partir de um desktop ou dispositivo portátil. O

portal pode ser usado para enviar solicitações de mudança de política, criar chamados, gerar relatórios e visualizar eventos de segurança e logs a partir de dispositivos gerenciados em um único local. Com o portal do SOC Virtual (ver Figura 7):

- Visualizações de segurança consolidadas possibilitam o monitoramento e o controle de todos os serviços de segurança gerenciados por meio de um centro de comando centralizado, bem como a visualização de todos os eventos de segurança e logs por meio de uma única interface com guias.
- Excelentes opções de consulta e relatório permitem consultas e relatórios ad hoc para dispositivos de segurança, eventos de segurança, atividade de acordo de nível de serviço e outros parâmetros, além de relatórios padrão customizados.
- Archives de evento/log fornecem armazenamento de evento/log online acessível por meio do portal do SOC Virtual e arquivamento offline no sistema de archives forense dos Serviços de Segurança IBM.
- Um sistema de permissões granular permite que você determine quem pode acessar o portal, o que cada usuário vê, o que cada usuário pode alterar e quem está autorizado a entrar em contato com o SOC.
- A integração de chamado de problema e fluxo de trabalho fornece um sistema de fluxo de trabalho de chamado de problema para a criação, designação e rastreamento do status dos chamados.
- A inteligência de segurança integrada da X-Force inclui feeds de inteligência de segurança integrada em tempo real da X-Force e ferramentas de pesquisa.

Gerenciamento e resolução de problemas

O processo para gerenciar incidentes de segurança é detalhado na Seção 3 deste guia. Os incidentes de serviço—problemas fora das operações de serviço padrão que causam, ou podem causar, uma redução na qualidade do serviço ou um comprometimento de segurança—são abordados por uma equipe separada de especialistas do SOC. Os dois tipos de incidentes são rastreados de ponta a ponta por meio do sistema integrado de chamados.

Incidentes de serviço classificados pelos clientes como graves (Gravidade 1) representam um risco para os processos de

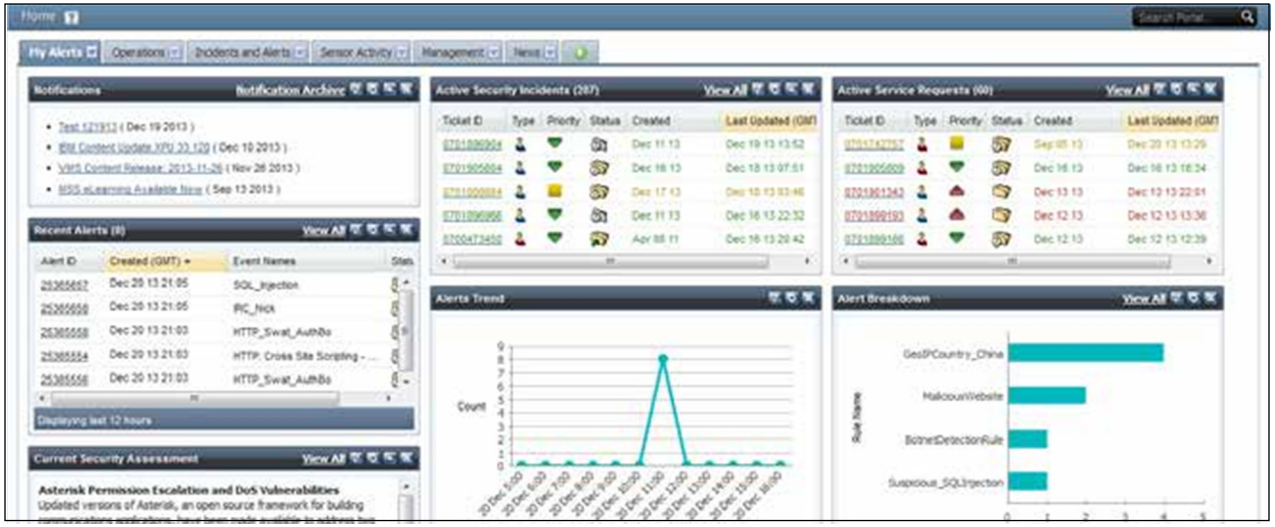


Figura 7. O portal do SOC Virtual oferece um ponto único de acesso para todos os aspectos da entrega dos Managed Security Services.

negócios essenciais, tais como geração de receita, ou resultam em indisponibilidade para um sistema, rede ou aplicativo importante que afeta a entrega de serviço de TI. Os incidentes graves são manipulados com um processo acelerado concebido para restaurar as operações normais o mais rapidamente possível. Os especialistas em gerenciamento de incidente do SOC trabalham com o cliente até a resolução do problema e, a qualquer momento, os clientes podem encaminhar a manipulação do problema ao líder ou gerente de turno da equipe do SOC.

Chamados de problema podem ser abertos para incidentes com prioridade mais baixa, seja por sistemas e funções de monitoramento automatizados, pela equipe do SOC ou por contatos de segurança do cliente. Esses problemas são encaminhados para as equipes de suporte às operações do SOC adequadas em busca de resolução.

Inteligência de segurança da X-Force

O IBM X-Force Threat Analysis Service está incluído com todos os Serviços de Segurança IBM e integrado no portal do SOC Virtual. Esse serviço de inteligência de segurança líder no setor ajuda você a gerenciar ameaças diárias de segurança proativamente, pois fornece uma avaliação de condições de ameaças online globais e análise detalhada adequada às suas necessidades. A Figura 8 mostra uma visualização do cliente comum da página inicial do X-Force Threat Analysis no portal do SOC Virtual, que oferece acesso rápido a:

- Current Security Assessment: um resumo dos eventos e liberações de produto importantes que poderiam afetar a segurança da sua rede
- Vulnerabilities: uma matriz customizada que mostra o número de vulnerabilidades, por categoria, durante os últimos 90 dias e desde seu último login no portal, bem como tendências em todos os dados de vulnerabilidade disponíveis

- **AlertCon 5-Day Forecast**: uma avaliação do nível de ameaça atual e antecipado de ataques online, indo do AlertCon 1 (vigilância regular necessária) ao AlertCon 4 (ameaça catastrófica iminente ou em curso)
- **Alerts/Advisories**: uma compilação em tempo hábil de informações recentes sobre novas ameaças da IBM e da US-CERT
- **Worms & Viruses**: os três worms e vírus mais ativos na Internet
- **Security News**: uma visualização agregada das notícias sobre segurança mais importantes compiladas pelo XFTAS, com links para um archive de notícias.

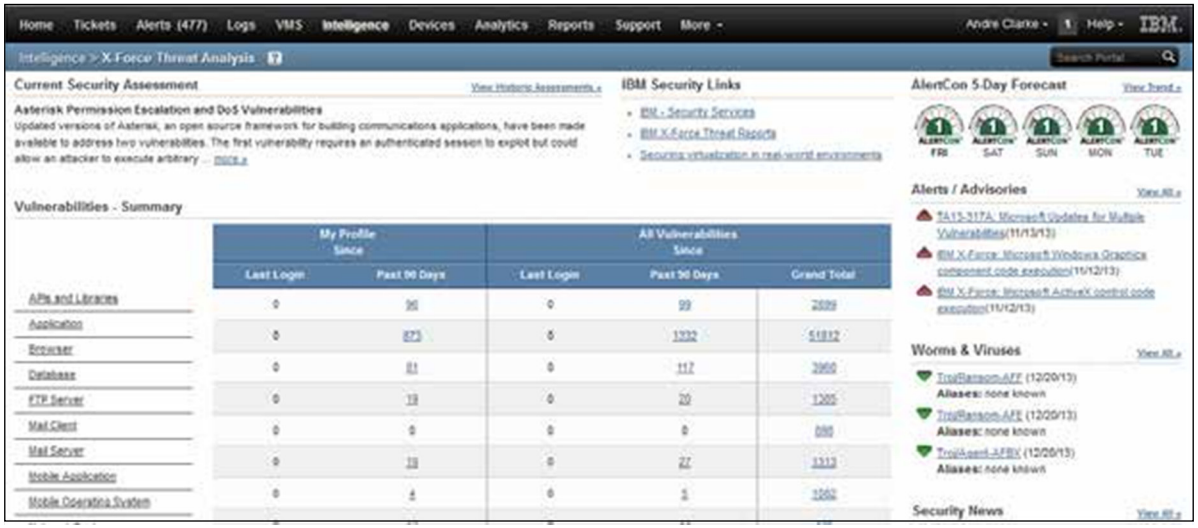


Figura 8. A página inicial do X-Force Threat Analysis Service oferece uma visão rápida de tendências de vulnerabilidade, status de segurança da Internet e sua avaliação de segurança customizada.

Notificação por email de avaliações e alertas de ameaças

Como cliente do XFTAS, é possível assinar newsletters diários que oferecem informações perspicazes sobre os problemas do dia, tendências de ameaças emergentes e seu impacto e uma lista customizada de vulnerabilidades, ameaças e artigos que são relevantes aos seus negócios. Também é possível assinar um email diário customizável de avaliação de ameaças que inclui indicativos de proteção da IBM e o status diário do AlertCon, que indica o estado atual de ameaça da Internet.

Relatórios padrão e customizados

A IBM fornece um mecanismo robusto de relatório e consulta que você pode usar para ajudar a facilitar operações diárias de segurança, incluindo pesquisa, avaliação de vulnerabilidade, mitigação de ameaças e priorização da carga de trabalho. Além disso, existem relatórios que podem ajudá-lo a gerenciar seus serviços IBM e abordar requisitos de conformidade de auditoria. A IBM fornece dados normalizados dos seus serviços e dispositivos IBM gerenciados e monitorados por ela.

Relatórios estão disponíveis 24 horas por dia, sete dias por semana por meio do Report Dashboard do portal do SOC Virtual (ver Figura 9). A IBM oferece vários modelos de relatório padrão do setor que você pode customizar por dispositivo, grupo de dispositivos ou prazo para corresponder aos seus requisitos. Além disso, é possível salvar seus critérios de relatório e agendar a execução automática de relatórios por hora, dia, semana, mês ou ano. Você pode visualizar os dados do relatório diretamente no portal ou exportar relatórios e enviá-los por email à sua comunidade de segurança em HTML, CSV, PDF ou outros formatos suportados.

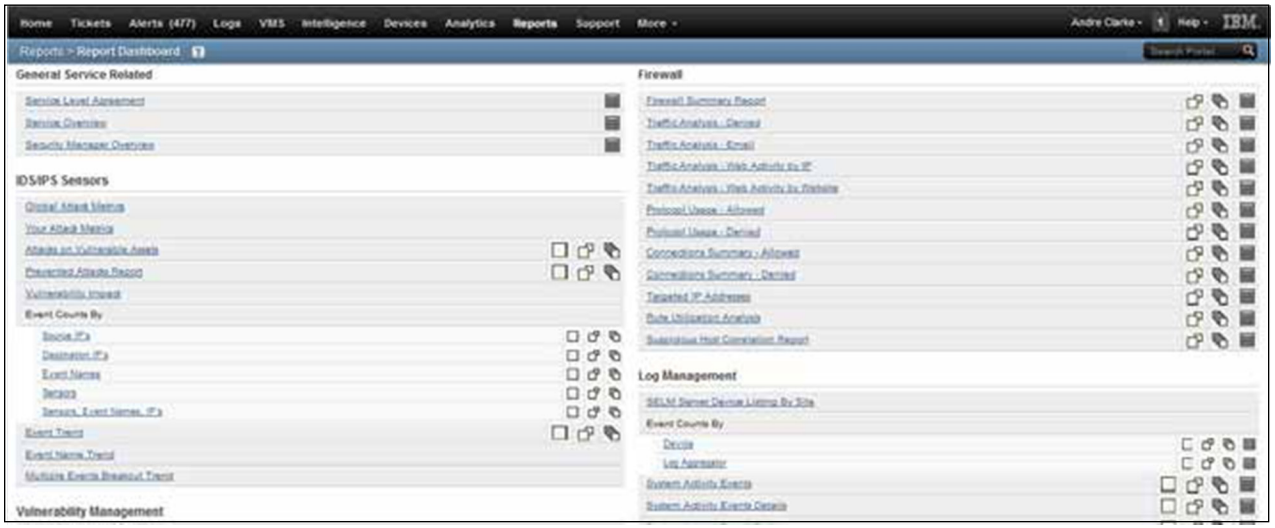


Figura 9. A seção Report Dashboard do portal do SOC Virtual fornece acesso imediato a todos os relatórios padrão e customizados em seu ambiente de segurança e serviços de segurança.

Para ajudá-lo a trabalhar de forma mais eficiente, os modelos de relatório são organizados nos seguintes grupos:

- **General Service Related**: Visão geral de eventos e incidentes e desempenho de serviço em geral
- **IDS/IPS Sensors**: Métricas de eventos detalhadas e tendências gerais de ataques detectadas por sensores
- **Vulnerability Management**: Dados de vulnerabilidade corporativa e de PCI para clientes que usam o Hosted Vulnerability Management Service

- **Firewall**: Dados detalhados relacionados a tráfego de rede, uso de protocolo, conexões, IPs de destino, utilização de regras e correlação de host suspeita
- **Log Management**: Dados de atividade do sistema para clientes usando o Hosted Security Event and Log Management Service
- **Alerts**: Resumos de possíveis problemas de segurança e contagens correspondentes
- **Content Management**: Filtragem de URL (o que foi bloqueado por categoria, por cliente e por IP de origem) e relatórios de antivírus
- **Compliance Reports**: Documentação do desempenho no cumprimento de normas regulamentares, do setor e jurídicas.

Como melhor prática, a IBM recomenda que os clientes executem e revisem regularmente os relatórios de contagem de evento, especialmente as contagens de evento por endereço de origem de IP, por nome do evento e por sensor. Juntos, esses relatórios podem ajudá-lo a determinar rapidamente se os ataques estão vindo de dentro ou de fora da sua organização, quais sistemas poderão ser comprometidos, quais tipos de ataques são mais predominantes e quais dispositivos poderão precisar de ajustes adicionais na política.

5. Próximos passos

Especialistas da IBM podem trabalhar com você para criar um business case que demonstre como os Serviços de Segurança IBM podem ajudá-lo a melhorar sua postura de segurança e mitigar os riscos para as operações de negócios, enquanto o custo e a complexidade do gerenciamento de segurança são reduzidos.

Contato

Se você quiser conversar com um representante dos Serviços de Segurança da IBM para discutir seus requisitos e objetivos de gerenciamento de segurança, entre em contato conosco diretamente pelo telefone 1-877-426-3287. Mencione o código 609CG98W (somente EUA e Canadá). Ou você pode nos enviar um email para solicitar uma resposta de um especialista da IBM.

Saiba mais

Leia sobre os problemas enfrentados por executivos de segurança de TI atualmente e como a IBM pode ajudá-lo a abordar seus desafios mais significativos.

Faça o download de IBM Security Services Cyber Security Intelligence Index para saber mais sobre as ameaças enfrentadas pela sua organização hoje em dia.

Leia o relatório da Forrester Surviving the Technical Security Skills Crisis para ter acesso à visão de analistas sobre a função dos serviços de segurança gerenciados no sentido de ajudar a preencher a lacuna de qualificações.

Compartilhe o relatório de Diretor de Segurança de Informações (CISO) intitulado A new standard for security leaders do IBM Center for Applied Insights.

Financiamento da IBM

A IBM Global Financing pode ajudá-lo a adquirir as soluções de TI de que seus negócios precisam da maneira mais econômica e estratégica possível. Trabalharemos com clientes com qualificação de crédito para customizar uma solução financeira de TI que se adapte às metas de negócios dos clientes, permita um gerenciamento de caixa efetivo e melhore o custo total de propriedade. A IBM Global Financing é a melhor opção para financiar investimentos importantes em TI e impulsionar seus negócios. Para obter mais informações, acesse: **ibm.com**/financing

Para obter mais informações

Para obter mais informações sobre os Serviços de Segurança da IBM, acesse nossa página da web: **ibm.com**/services/security

Siga-nos

IBM Global Services
Route 100
Somers, NY 10589
EUA

Produzido nos Estados Unidos da
América – Janeiro de 2014

Este documento é atual na data inicial de publicação, podendo ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países em que a IBM atua.

AS INFORMAÇÕES CONTIDAS NESTE DOCUMENTO SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM", SEM GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUSIVE SEM GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM PROPÓSITO ESPECÍFICO E GARANTIA OU CONDIÇÃO DE NÃO VIOLAÇÃO. Os produtos IBM possuem garantia de acordo com os termos e condições dos contratos conforme os quais são fornecidos.

O cliente é responsável por assegurar o cumprimento das leis e regulamentos aplicáveis a ele. A IBM não oferece assessoria jurídica nem declara ou garante que seus serviços ou produtos assegurarão que o cliente esteja cumprindo qualquer lei ou regulamento.

As ofertas da IBM Global Financing são feitas por meio da IBM Credit LLC nos Estados Unidos e de outras subsidiárias e divisões da IBM no mundo todo para clientes comerciais e do governo qualificados. Os preços e a disponibilidade são baseados na classificação de crédito de um cliente, nos termos de financiamento, tipo de oferta, tipo de equipamento e produto e opções, podendo variar por país. Os itens que não são de hardware devem ser encargos únicos não recorrentes, financiados por meio de empréstimos. Outras restrições podem ser aplicadas. Os preços e as ofertas estão sujeitos a mudança, prorrogação ou cancelamento sem aviso prévio e podem não estar disponíveis em todos os países.

Declaração de Boas Práticas de Segurança: A segurança do sistema de TI envolve a proteção de sistemas e informações por meio da prevenção, detecção e resposta ao acesso indevido dentro e fora da sua empresa. O acesso indevido pode resultar na alteração, destruição ou uso indevido de informações, assim como em danos a seus sistemas ou uso indevido dos mesmos, inclusive em ataques a terceiros. Nenhum sistema ou produto de TI deve ser considerado totalmente seguro e nenhum produto, serviço ou medida de segurança pode ser totalmente eficaz para prevenir o uso ou acesso indevido. Os sistemas, produtos e serviços IBM são concebidos para fazerem parte de uma abordagem abrangente de segurança, o que necessariamente envolverá procedimentos operacionais adicionais e pode exigir que outros sistemas, produtos ou serviços sejam mais eficazes. A IBM NÃO GARANTE QUE SEUS SISTEMAS, PRODUTOS OU SERVIÇOS ESTÃO IMUNES A, OU TORNARÃO SUA EMPRESA IMUNE A, CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PARTE.

Recicle

SEO03083-BRPT-01