# FIREEYE SECURITY ORCHESTRATOR

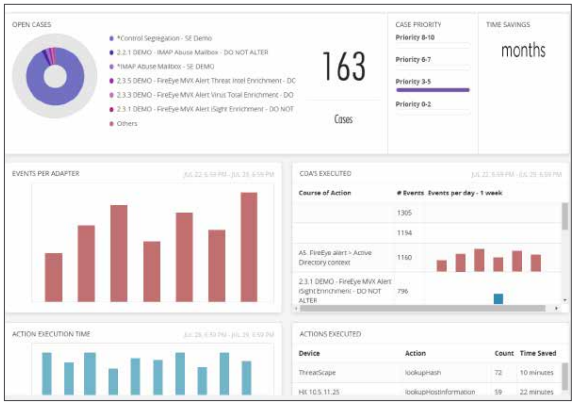
INTEGRE E AUTOMATIZE TECNOLOGIAS E PROCESSOS DE TRATAMENTO DE INCIDENTES PELA SUA INFRAESTRUTURA DE TI

## VISÃO GERAL

O volume de ataques cibernéticos nunca foi tão grande e se as suas defesas não conseguem acompanhar a tendência, o risco de violação aumenta drasticamente. Os atacantes dispõem dos recursos intelectuais, do poder computacional e do backbone das mais rápidas redes de entrega digital. Eles podem realizar iterações nas suas defesas à vontade, mudando a assinatura de ataque, adotando novos métodos de entrega e modificando constantemente a abordagem à questão de como infiltrar a sua rede. Eles podem fazer tudo isso o dia todo, todos os dias. Quando levamos em consideração o volume de alertas processado diariamente pela maioria dos centros de operações de segurança (SOCs) e o fato de que não se encontram os recursos necessários para operar esses centros, um programa tradicional que se baseie em intervenção e contenção manuais enfrenta uma batalha assimétrica.

O FireEye Security Orchestrator acelera e simplifica o processo de detecção e resposta a ameaças ao unificar tecnologias e processos de tratamento de incidentes separados em um único console que proporcione respostas orientadas em tempo real para melhorar os tempos de resposta, reduzir a exposição ao risco e manter a consistência dos processos dentro de um programa de segurança. Os anos de experiência da FireEye combatendo as violações de maior repercussão do mundo contribuíram para o aperfeiçoamento de processos eficazes de detecção, investigação e resposta a ameaças. O FireEye Security Orchestrator permite sobrepor essas melhores práticas aos dados da sua distribuição FireEye, ao seu SIEM e a outras tecnologias corporativas.

O FireEye Security Orchestrator pode promover mudanças em nível de rede, de host e de aplicativo, e até mesmo em sistemas de controle de acesso. A capacidade de responder em meros segundos detém, efetivamente, os intrusos e fecha-lhes as portas,




## VANTAGENS

- Melhore a capacidade da equipe de segurança com roteiros predefinidos, criados e distribuídos por uma equipe com visibilidade de décadas nas linhas de frente das principais investigações de ataques cibernéticos.
- Elimine erros através de automação e processos padronizados, além de reduzir os requisitos de tempo das já sobrecarregadas equipes do SOC.
- Permita que as equipes do SOC reduzam o risco com tempos de resposta menores, possibilitando que se concentrem em tarefas de prioridade mais alta que possam aprimorar ainda mais a sua postura de risco — por exemplo, caça.
- Dashboards e gerenciamento de casos centralizados para ancorar o processo das suas operações de segurança.

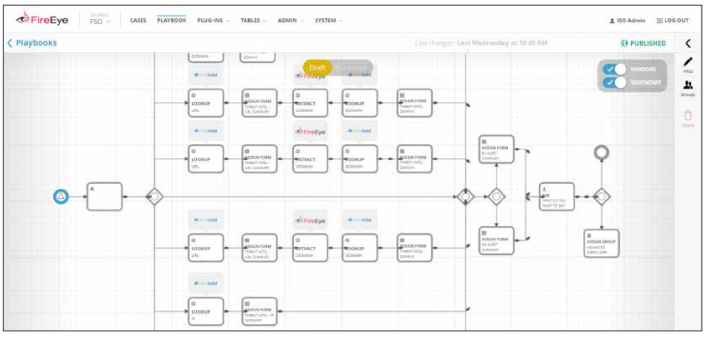
limitando os danos e o risco para a organização. Com o FireEye Security Orchestrator, você poupa tempo e recursos ao unificar dados relacionados a incidentes e as suas tecnologias de segurança sob uma mesma plataforma de operações de segurança.

Nossos clientes reduzem significativamente os tempos de resposta, eliminam erros de processos e, com isso, reduzem sua exposição geral ao risco.

## PRINCIPAIS RECURSOS

### Roteiros de resposta a incidentes

Os roteiros de resposta a incidentes, também conhecidos como cursos de ação (CoAs), codificam as operações de segurança em tarefas automatizadas e fluxos de trabalho liderados por humanos. Com seus processos de SOC documentados, automatizados e aprimorados com os conhecimentos da FireEye no combate aos ataques mais avançados do mundo, os seus tempos de resposta diminuirão, enquanto a consistência do processo é mantida dentro de um programa de segurança.




Use o novo construtor de CoA para criar fluxos de trabalho ramificados e inteligentes que coincidam com a forma como a política de segurança e a infraestrutura de suporte da sua organização funcionam. Ele é fornecido com um portfólio completo de plug-ins e fluxos de trabalho predefinidos para as ferramentas de suas operações de segurança, como SIEM, firewall, inteligência sobre ameaças, IPS e sistemas de tiquetagem. Em seguida, ele permite a criação de fluxos de trabalho personalizados de acordo com as políticas de segurança e com a infraestrutura de suporte da sua organização. Com roteiros, você pode desconstruir os fluxos de trabalho dos analistas de segurança em uma sequência total ou parcialmente automatizada de tarefas, com a possibilidade de solicitar feedback de analistas para informar a direção de um determinado fluxo de trabalho. O resultado final será um ambiente de funcionamento harmônico, com fluxos de trabalho de segurança desenvolvidos e aprovados pela sua organização. Essas mudanças serão transformadas em fluxos de trabalho de automação que podem ser iniciados automaticamente, desencadeados por eventos da sua infraestrutura ou executados conforme a necessidade pela equipe do seu SOC.

### Acesso com base em funções

Crie grupos com base em funções e atribua permissões granulares a roteiros individuais ou a etapas específicas dentro do roteiro. Dessa forma, cada equipe tem acesso para execução e privilégios para ler os resultados apenas dos fluxos de trabalhos necessários. Você pode utilizar grupos ou usuários locais ou integrar o seu Active Directory ou diretório Open LDAP e atribuí-los a funções no Orchestrator.

### Plug-ins

Integre, unifique e controle a sua infraestrutura de TI a partir de um único painel, por meio da estrutura de trabalho do plug-in. Os plug-ins são a malha de conexão que reúne os seus dispositivos, aplicativos, serviços e dados no FireEye Security Orchestrator. Eles são construídos com suporte para algumas das tecnologias de infraestrutura e segurança mais populares.

Essa arquitetura com base em plug-ins permite que as organizações troquem ou adicionem tecnologias com o mínimo de integração e treinamento de resposta. Os plug-ins têm capacidade de comando e controle bidirecional para o recebimento de dados e a tomada de providências.

### Dashboards personalizados e caça avançada

O FireEye Security Orchestrator oferece um dashboard investigativo para pesquisar por ferramentas de segurança e viabilizar a caça aos perpetradores de ameaças que visaram a sua organização. Você também pode gerenciar casos e alternar rapidamente de roteiros para contexto adicional pela infraestrutura de segurança existente.

Além disso, seus analistas também podem visualizar um dashboard centralizado e mapas de ameaças mundiais para criar uma visualização de ponta a ponta dos dados e ataques detectados pelos appliances da FireEye dentro da sua organização. Essa visualização pode proporcionar a você insights, tanto históricos quanto em tempo real, para ajudar a promover detecção e resposta

rápidas. Também é possível realizar investigações profundas por meio de pesquisas ultrarrápidas, em camadas e altamente flexíveis nos dados de notificação de alertas da FireEye. Isso permite alternar rapidamente de um alerta para o contexto maior por trás do ataque. Todos os dashboards de pesquisa também podem ser salvos e enviados por e-mail.


**Relatórios**

Você pode criar relatórios únicos ou recorrentes que detalhem, correlacionem e apresentem alertas relacionados. As equipes de segurança podem determinar rapidamente as origens, a metodologia e os alvos de um ataque e evitar recorrências futuras. Os relatórios podem ser personalizados com:

- Milhares de parâmetros de alerta
- Filtros cirúrgicos
- Vários formatos de arquivo
- Temas com gráficos específicos da organização
- Serviços profissionais: orquestração

Serviços de distribuição personalizados estão disponíveis para projetar e distribuir o FireEye Security Orchestrator no seu programa e na sua arquitetura de segurança. Esses serviços aproveitam o conhecimento da FireEye para criar os roteiros apropriados com base nas soluções de tecnologia do seu ambiente e nas ameaças que a sua organização enfrenta todo dia.

Para obter mais informações sobre a FireEye, visite:
**www.FireEye.com**

**SOBRE A FIREEYE, INC.**

A FireEye é líder em segurança como serviço (SaaS) orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência sobre ameaças em nível de país e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos. A FireEye tem mais de 5.000 clientes em 67 países, incluindo mais de 940 empresas da Forbes Global 2000.

**FireEye, Inc.**
1440 McCarthy Blvd. Milpitas, CA 95035
+1 408.321.6300 / 877.FIREEYE (347.3393) / LATAM@FireEye.com

**www.FireEye.com**

© 2016 FireEye, Inc. Todos os direitos reservados. FireEye é uma marca registrada da FireEye, Inc. Todos os outros nomes de marcas, produtos e serviços são ou podem ser marcas comerciais ou marcas de serviços de seus respectivos proprietários. DS.FSO.PT-BR.052016

FireEye