DETECÇÃO E RESPOSTA GERENCIADA DO ACTIVEEYE

UMA VISÃO GERAL TÉCNICA

MOTOROLA SOLUTIONS

DETECÇÃO E RESPOSTA GERENCIADA DO ACTIVEEYE

O ActiveEye℠ Managed Detection and Response (MDR) aproveita nossa avançada plataforma de segurança ActiveEye e analista experiente para detectar e responder a ameaças cibernéticas no ambiente de TI, bem como despacho auxiliado por computador (CAD), sistemas VESTA© 9-1-1 e ASTRO© 25 Sistemas. Este informe técnico fornece uma visão geral técnica de nossos serviços e da plataforma ActiveEye.

COMPONENTES DO MDR DO ACTIVEEYE

Plataforma ActiveEye Security Management

ActiveEye é uma orquestração, automação e resposta de segurança (SOAR) que serve como o coração das operações de segurança. A plataforma ActiveEye ingere dados de elementos de rede conectados, analisa-os e envia dados e insights relevantes para o pessoal de segurança cibernética. A análise e a filtragem ajudam a diferenciar entre tráfego malicioso e rotineiro, simplificando o foco nas ameaças reais. Os seguintes módulos de detecção de ameaças estão disponíveis na plataforma ActiveEye:

- Análise de Registros
- Detecção de Rede
- Detecção e Resposta de Endpoint (EDR)
- Detecção de DNS
- Detecção de Vulnerabilidade

Essa plataforma ActiveEye coleta e gerencia dados de segurança, otimizando a detecção de ameaças e aumentando o foco nos alertas mais críticos que exigem respostas rápidas. Os recursos de análise integrados examinam vários feeds de inteligência de ameaças em tempo real, fazem referência a eventos passados e seguem os manuais definidos para automatizar a maioria das ações dos analistas. O Analytics também classifica as investigações manuais, priorizando aquelas com maior probabilidade de exigir correção.

Sensor de segurança remoto ActiveEye ("ActiveEye Remote Security Sensor" - AERSS)

O AERSS é um componente opcionalmente implantado que fornece coleta remota de logs, detecção de intrusão de rede e verificação de vulnerabilidades.

Centro de Operações de Segurança (SOC)

Os experientes analistas de segurança cibernética da Motorola Solutions monitoram 24 horas por dia, 7 dias por semana, em busca de possíveis ameaças. Os analistas alertam os principais contatos de sua organização para mobilizar uma resposta e fazem contatos de sua organização para mobilizar uma resposta e fazer recomendações com base em um plano de ação predefinido se detectarem uma ameaça. Os serviços SOC padrão podem ser aprimorados com nosso serviço opcional Advanced Threat Insights, que fornece equipe de contas dedicada e busca proativa de ameaças.

PLATAFORMA DE GESTÃO DE SEGURANÇA ACTIVEEYE

O ActiveEye é rápido e simples de implantar, eliminando a carga de instalação, manutenção e gerenciamento de um componente de gerenciamento de eventos e informações de segurança (SIEM) no local. Dependendo das fontes de log que precisam ser monitoradas, o ActiveEye pode substituir a necessidade de um SIEM separado. O acesso e o conteúdo do ActiveEye são protegidos por poderosas funções de segurança. Os usuários acessam a plataforma por meio de um navegador da Web seguro usando autenticação multifator (MFA). As funções administrativas permitem gerenciar o acesso do usuário conforme necessário.

A plataforma passa por auditorias de segurança regulares e possui uma certificação de auditoria SOC 2 Type2 ativa. Usamos as melhores práticas de segurança de dados para criptografar dados em trânsito de/para a plataforma e em repouso. Os dados de nível de alerta e evento Aw são armazenados por 13 meses por padrão e podem ser armazenados por mais tempo, se necessário.
Existem vários "pods" ActiveEye, locais independentes implantados em todo o mundo, incluindo EUA, GovCloud dos EUA, Canadá e Austrália.

INTELIGÊNCIA DE AMEAÇAS E ENRIQUECIMENTO DE DADOS

O ActiveEye usa inteligência de ameaças para detecção de ameaças e enriquecimento de alertas. As fontes de inteligência de ameaças são cuidadosamente selecionadas por especialistas em domínio de segurança que monitoram a infraestrutura de comando e controle e outras entidades relevantes. Essa curadoria garante que novas ameaças sejam detectadas e tratadas o mais rápido possível após o anúncio de uma vulnerabilidade ou ameaça. Coletivamente, a inteligência de ameaças no ActiveEye é derivada de várias fontes, incluindo:

- Inteligência expansiva de código aberto (OSINT) que incorpora várias fontes menores.
- Fontes comerciais pagas que permitem dados agregados e informações sob demanda sobre entidades como arquivos ou IPs.
- Dados derivados dos especialistas do ActiveEye SOC à medida que navegam em dezenas de milhares de alertas por dia.

Além disso, a Motorola Solutions desenvolve e mantém uma ampla inteligência de ameaças específicas do setor para governos estaduais e locais, segurança pública e grandes empresas.

DETECÇÃO DE AMEAÇAS

A plataforma ActiveEye maximiza o valor das detecções fornecidas por serviços de segurança integrados, como provedores de detecção e resposta de endpoint (EDR) de última geração. Ele também oferece detecções personalizadas em serviços que fornecem apenas logs, como muitos SaaS e plataformas de nuvem. Em ambos os casos, os dados brutos de eventos são ingeridos no ActiveEye e analisados por centenas de políticas que analisam os dados para descobrir anomalias, famílias de malware conhecidas e outros riscos.

Para fornecedores que fornecem detecções, as políticas do ActiveEye enriquecem os alertas recebidos com taxonomia de alerta, aprendizado de máquina (ML) – gravidades derivadas e outros metadados. Os alertas também podem ser correlacionados a outros dados relevantes para expor relacionamentos ocultos, enriquecidos com inteligência de ameaças e modificados com base no comportamento histórico.

Para integrações de log sem alerta integrado, o mesmo processo se aplica. No entanto, as políticas operam nos dados brutos para descobrir que o limite está sendo violado, padrões de risco conhecidos e outras condições que exigem investigação. Assim como os alertas derivados do fornecedor, os dados resultantes são enriquecidos e correlacionados antes de serem triados.

Todas as políticas são executadas como processos de streaming, assim que os dados chegam, e também como uma verificação histórica para identificar agregados que podem ser perdidos no processo de streaming sem estado. A lista completa de políticas aplicáveis pode ser revisada na interface do ActiveEye.

ORQUESTRAÇÃO E AUTOMAÇÃO DE SEGURANÇA

Como uma plataforma SOAR, o ActiveEye orquestra o fluxo de dados e ações, acelerando a correção por meio da execução automática de tarefas de investigação e resposta. Usando playbooks predefinidos ou personalizados, o ActiveEye lida com tarefas repetitivas e precisas no lugar de analistas SOC humanos. ActiveEye suporta dois tipos de automação:

- Automação de Enriquecimento e Investigação – O ActiveEye pode analisar sua inteligência de ameaças, consultar dados anteriores e exibir detalhes de eventos na tela principal de investigação. Esses dados melhoram a qualidade e a velocidade da investigação manual e fornecem uma base sobre a qual a automação pode tomar decisões.

- Automação de resposta – o ActiveEye pode executar a ação de resposta definida nos manuais. As ações podem incluir fazer recomendações aos analistas, alterar a prioridade do alerta, fechar um alerta, bloquear arquivos, remover arquivos de sistemas ou isolar um host da rede.

PORTAL DE SEGURANÇA CO-GERENCIADO ACTIVEEYE

Como uma plataforma cogerenciada, o ActiveEye sincroniza os esforços de segurança entre sua equipe de segurança e nossos analistas de SOC. O portal baseado na web forneceu visibilidade para insights de ameaças, investigações de eventos, relatórios de segurança, avisos de ameaças e o status de quaisquer casos de segurança.

Painel

As principais informações do portal ActiveEye são resumidas no painel. Esse painel inclui alertas abertos, uma visão geral das categorias de alertas, indicadores chave de desempenho (KPI) de processamento de alertas, casos de segurança abertos e alertas recentes sobre ameaças. A partir daqui os usuários podem acessar informações mais detalhadas, como casos de segurança, detalhes de alertas, tendências de alertas, relatórios e comunicações em grupo.

Casos de segurança

Quando a Motorola Solutions identifica uma ameaça, o SOC cria um caso de segurança. Os casos de segurança podem ser visualizados no portal ActiveEye e podem ser resumidos em um Resumo de Segurança Diário opcional enviado por e-mail.

Detalhes e tendências do alerta

Alertas são notificações do sistema de atividades incomuns. Esses alertas podem ser uma evidência de uma ameaça ativa ou em desenvolvimento no passado. Se os analistas acreditam que os alertas são indicativos de uma ameaça, eles podem abrir casos de segurança com base neles.
O ActiveEye registra dados relevantes para cada alerta, permitindo que os usuários visualizem rapidamente seus acionadores, sistemas que impactam e quaisquer ações tomadas para abordá-lo. Cada registro de alerta também inclui um resumo dos principais atributos. A partir desse resumo de alertas, os usuários podem acessar os registros relacionados para obter mais detalhes. Esses registros incluem inteligência de ameaças, dados de eventos passados, eventos relacionados e logs de atividades.

Para contextualizar os alertas, o ActiveEye forneceu ferramentas para revisar grupos de alertas com base em atributos-chave ou períodos de tempo. Os filtros de atributo permitem que os usuários alternem quais grupos de alertas o ActiveEye mostra, ajudando a identificar tendências ou atividades de ameaças. Os usuários também podem comparar os logs de alerta por períodos de tempo para determinar se as tendências associadas a uma ameaça ou são falsos positivos.

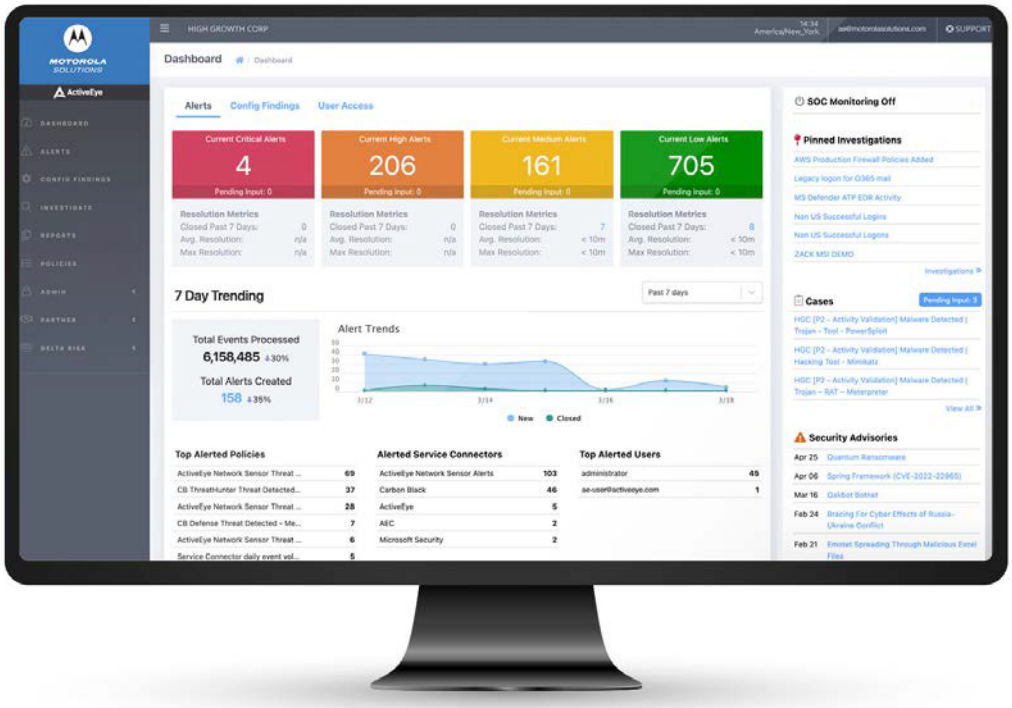


Figura 1-1: Interface ActiveEye

Investigações e Relatórios

Os recursos robustos e ad hoc de relatórios do ActiveEye permitem que os usuários investiguem e procurem por ameaças ativas e visualizem conjuntos de dados históricos. Os relatórios fornecem uma visão simples e consistente dos dados de eventos coletados. Os modelos predefinidos organizam os dados e exibem os atributos mais importantes dos tipos de eventos. Os usuários podem personalizar esses relatórios padrão para exibir e resumir diferentes atributos quando necessário. Para compartilhar informações fora do ActiveEye, os usuários podem baixar relatórios de até 50.000 linhas no formato .cvs js.

Além de relatórios e consultas ad hoc, o ActiveEye pode fornecer relatórios mensais opcionais e resumos diários via e-mail. O relatório mensal resume itens importantes de segurança e está disponível como um conjunto de estatísticas do dia anterior para uma lista de usuários predeterminada. Esse resumo pode incluir contagens de alertas, casos de segurança abertos/fechados, consultas salvas com novos dados e estatísticas de segurança detalhada de endpoint. O ActiveEye pode enviar um ou mais e-mails de resumo com conteúdo diferente para grupos diferentes.

Avisos de Segurança

Os Avisos de Segurança são mensagens ao SOC com informações sobre ameaças ativas para a população em geral ou seu setor específico. Esses avisos orientam as equipes de segurança sobre a melhor forma de agir contra uma ameaça e informam onde podem encontrar mais informações.

Compartilhamento de Informações

Para oferecer suporte ao gerenciamento de segurança eficaz, o ActiveEye possui várias funções para compartilhar informações. Alertas de segurança automáticos notificam os principais contatos sobre incidentes com base na prioridade. Além dos alertas de segurança automáticos, o ActiveEye apresenta as funções de compartilhamento de informações que você e a equipe de SOC da Motorola Solutions podem acessar, incluindo:

- **Boletins SOC** – Instruções de sua equipe de segurança ou do SOC que os analistas SOC podem consultar ao criar casos de segurança. Eles podem comunicar situações de curto prazo em que um caso de segurança pode não ser necessário, como durante testes ou janelas de manutenção.
- **Caderno do Cliente** – O SOC pode usar o Caderno do Cliente para documentar detalhes sobre seu ambiente específico e informações de implementação de rede para ajudar nossos analistas a investigar casos de segurança.
- **Procedimentos de contato** – procedimentos de encaminhamento e instruções sobre quem contatar se ocorrer um incidente também estão prontamente disponíveis. Os procedimentos de contato incluem instruções e procedimentos para níveis específicos de incidentes de segurança. O SOC e o cliente gerenciarão em conjunto os procedimentos de contato.

Juntas, essas funções espalham rapidamente informações importantes para equipes e analistas de segurança.

Acesso do Usuário ao ActiveEye

As configurações de acesso do usuário simplificam a adição, atualização e remoção do acesso ao ActiveEye. Cada usuário do ActiveEye pode salvar consultas, personalizar relatórios e configurar resumos diários por e-mail. Os usuários personalizam relatórios e configuram resumos diários por e-mail. Os usuários podem receber acesso administrativo, permitindo que eles executem tarefas administrativas, como configurar novos conectores de serviço, redefinir senhas e configurar autenticação multifator para outros usuários.

MÓDULOS DE DETECÇÃO DE AMEAÇAS ACTIVEEYE

Análise de Registro

A função Análise de Registro coleta dados de sistemas, aplicativos, componentes de rede, sistemas de segurança e até mesmo outras soluções SIEM. Vários componentes de análise e políticas de segurança processam a data do log para identificar violações de política e atividades suspeitas. Se o ActiveEye detectar um evento de interesse que possa representar uma ameaça, ele alertará os analistas com base em suas configurações.

Com o tempo, os eventos registrados no passado podem fornecer um contexto crítico para rastrear a origem de uma ameaça ou identificar uma nova ameaça usando padrões de ataque anteriores. O ActiveEye armazena eventos coletados para que os analistas possam pesquisá-los e usá-los para caçar ameaças. Os eventos permanecem armazenados por um período de tempo definido com base na assinatura. Embora o prazo padrão seja de um ano, períodos mais longos estão disponíveis por assinatura.

O ActiveEye pode incorporar uma variedade de logs de diferentes fontes, incluindo sistemas de autenticação e autorização, armazenamento de objetos, redes virtuais em nuvem, servidores virtuais, serviços de segurança em nuvem, aplicativos de software e infraestrutura física via AERRS.

Detecção de Rede

O módulo de serviço Network Detection usa uma abordagem sem agente para monitorar todas as atividades na rede, fornecendo visibilidade de quais dispositivos estão conectados e quais aplicativos estão se comunicando de cada dispositivo. Com a integração do ActiveEye, as equipes de segurança podem automatizar a investigação de alertas de tráfego de rede e visualizar esses alertas no contexto de outras atividades do usuário. Além de alertar sobre indicadores de reconhecimento ou comprometimento ativo, a investigação do ActiveEye rastreia facilmente o comportamento que não é capturado por assinaturas de tráfego predefinidas, incluindo atividade em conexões criptografadas.

O conjunto de assinaturas do módulo Network Detection é atualizado a cada hora, garantindo que as ameaças sejam tratadas assim que a comunidade de segurança cibernética souber sobre elas.

Detecção e Resposta de Endpoint

Se um invasor tentar violar a segurança, é fundamental poder responder mais rapidamente. A integração das ferramentas Endpoint and Response (EDR) com a plataforma ActiveEye permite que os analistas de segurança respondam a ataques e visualizem a inteligência de ameaças em uma interface. Isso permite que eles reajam rapidamente a uma emergência, em vez de precisar alternar entre ferramentas separadas para investigar e combater um ataque.

Os analistas podem acessar uma variedade de ações de resposta no ActiveEye, como isolar hosts, bloquear arquivos, permitir e remover arquivos. As respostas disponíveis são determinadas pela ferramenta EDR e pelas políticas de segurança. Se o cliente não tiver uma solução EDR, a Motorola Solutions poderá recomendar ou fornecer uma como parte deste serviço por um custo adicional.

Detecção de DNS

As redes de computadores usam o Domain Name System, ou DNS, para traduzir nomes de domínio em endereços IP que os computadores usam para se comunicarem. Nosso recurso de detecção de DNS emprega um serviço de resolução de DNS com reconhecimento de segurança para evitar que malware, botnets e ataques de phishing comprometam sistemas e removam dados. Para evitar a perda de dados, o serviço pode bloquear a remoção ou transferência de dados por meio de portas ou protocolos de redes específicos. Isso pode impedir que um invasor ou usuário não autorizado remova dados, independentemente de iniciar o ataque com uma solicitação de DNS ou tentar contornar o DNS com uma conexão IP direta. Ele também pode bloquear a transferência de dados iniciada dentro ou fora de sua rede, impedindo a resolução de DNS para destinos potencialmente maliciosos.

Uma vez integrado com a plataforma ActiveEye, o DNS Detection alertará para sistemas que tentam acessar destinos maliciosos conhecidos ou destinos bloqueados pelas políticas de segurança de nossa organização. O serviço também permite visualizar e baixar relatórios de tendências de uso por categorias ou sistemas individuais.

Algumas configurações de DNS podem precisar variar de acordo com a localização de um dispositivo. A detecção de DNS pode ser personalizada com políticas de reconhecimento de local (em qual rede o sistema está) que bloqueiam ou permitem o tráfego com base em listas predefinidas.
A detecção de DNS geralmente é integrada ao perímetro da rede, protegendo os dispositivos dessa rede. Ao instalar um agente de software em dispositivos móveis aplicáveis, você pode estender a proteção DNS nesses dispositivos para fora do perímetro da rede. A Detecção de DNS pode impor proteções exclusivas nesses dispositivos, com restrições de acesso à Internet e configurações de registro variadas, caso estejam fora de sua rede.

Detecção de Vulnerabilidade

Durante a configuração ou atualizações do sistema, algumas configurações, softwares ou atualizações podem criar inadvertidamente uma abertura na segurança. O módulo de serviço de Detecção de Vulnerabilidades conecta ferramentas de terceiros com o ActiveEye para que ele possa destacar essas vulnerabilidades para proteger contra ameaças cibernéticas como ransonware, violações e perda de disponibilidade.

A função de detecção de vulnerabilidades verificará regularmente redes e sistemas configurados em busca de novas vulnerabilidades de componentes de software e configurações inseguras de sistema ou rede. Um mecanismo de verificação baseado em nuvem verificará pontos de extremidade acessíveis à Internet vulneráveis, enquanto o AERRS verificará a infraestrutura local. A Motorola Solutions trabalha com sua equipe para determinar a programação e o escopo de varredura ideais para o sistema.
As verificações concluídas resumirão todas as vulnerabilidades detectadas, juntamente com as ações recomendadas para fechá-las. As verificações pontuarão as vulnerabilidades detectadas usando o Common Vulnerability Scoring System, identificarão se elas estão em uma lista de Vulnerabilidades e exposições comuns e listarão os hosts afetados.

SENSOR DE SEGURANÇA REMOTO DO ACTIVEEYE

O Sensor de Segurança Remoto do ActiveEye (AERSS) é um servidor montado em rack implantado em seu ambiente. Ele coleta e monitora logs relevantes de segurança e tráfego de rede e reporta para a plataforma ActiveEye. Para a configuração de gerenciamento inicial, o AERSS será configurado usando ferramentas de linha de comando.

Após a configuração inicial, o AERSS é uma caixa autogerenciada; todas as atualizações dos componentes e do sistema operacional são executadas automaticamente em segundo plano. O acesso remoto é necessário em alguns casos para manutenção completa do sistema. Normalmente, nenhuma ação adicional da equipe local é necessária.

COLOCAÇÃO DA REDE AERSS

O monitoramento da rede é uma das principais funções do AERRS. Um dispositivo AERSS observa o tráfego que passa por vários pontos da rede para verificar se há atividades maliciosas. As considerações sobre onde conectar a porta de monitoramento seriam:

- Interfaces internas de firewalls de perímetro para permitir que eles bloqueiem o "ruído" excessivo da internet para que apenas o tráfego de passagem seja monitorado.

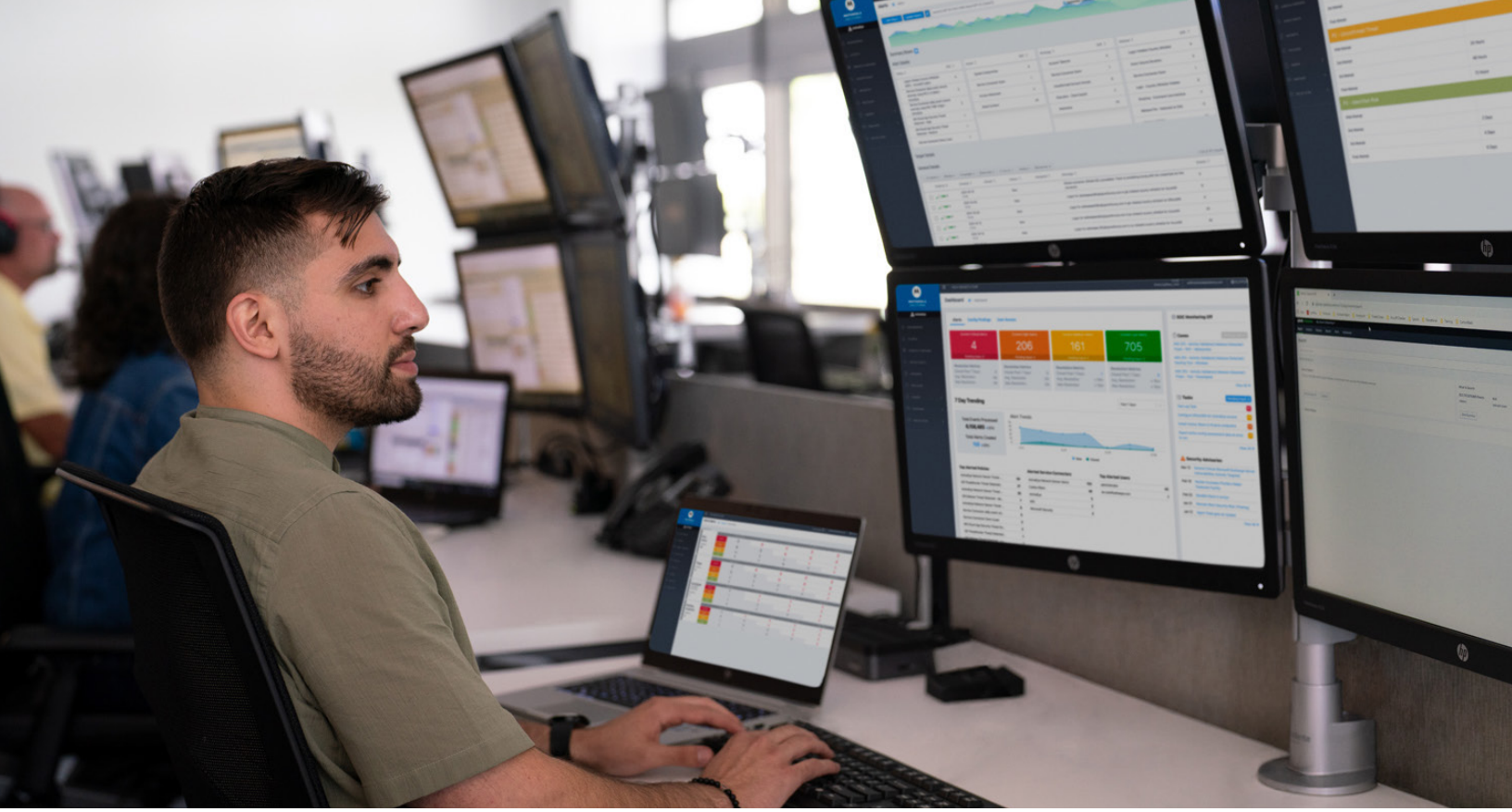
- Redes internas e servidores contendo dados confidenciais para garantir que as comunicações entre esses sistemas ou outros pontos de estrangulamento internos na rede, incluindo conexões de escritório ou parceiro/fornecedor, sejam monitoradas.

Outra consideração seria coletar logs de dispositivos dentro da rede. Os sistemas ou dispositivos de rede normalmente encaminham logs via syslog para o dispositivo AERSS para coleta e encaminhamento para o ActiveEye.

A última consideração seria para a varredura de rede em ambientes aplicáveis. Isso exigia que um dispositivo AERSS verificasse a rede em busca de vulnerabilidades. As considerações sobre onde conectar a porta de gerenciamento seriam:

- Um local dentro da rede, para facilitar a verificação sem alterar os controles de rede que seriam necessários durante a verificação por meio de firewalls ou outros controles de segurança que possam afetar a verificação.

- Para maior segurança, a porta de gerenciamento pode ser mais isolada. Nesse caso, uma configuração precisa do tráfego de saída para verificar as redes desejadas é necessária para a configuração. Isso é necessário para que a descoberta de varredura e outras verificações identifiquem corretamente os sistemas ativos nas redes, em vez de falsos positivos.



USO DA LARGURA DE BANDA AERSS

O dispositivo AERSS usa largura de banda para diversas finalidades. Pode afetar a rede em ambientes com largura de banda limitada. A principal consideração de largura de banda é para a internet, que é processada pela instalação, administração e conexão de log do dispositivo de AERSS. No mínimo, o appliance deve ter uma conexão de 10 Mbps à Internet disponível.

Secundariamente, há considerações de largura de banda dentro da rede que podem afetar o número ou o posicionamento dos dispositivos AERSS. As seguintes funções podem afetar os requisitos de largura de banda internos ao ambiente:

- Coleta de registros de dispositivos – A entrega de registros de dispositivos do outro lado de uma conexão de rede de baixa largura de banda pode ser afetada.
- Varredura de rede – A varredura de uma rede com uma conexão de baixa largura de banda pode aumentar os tempos de varredura ou afetar outro tráfego usando essa conexão.
- Monitoramento de rede – Se o tráfego de rede que está sendo replicado para monitoramento não estiver usando uma conexão dedicada, isso poderá afetar outro tráfego. Recomendamos sempre usar uma conexão dedicada e direta do switch replicando o tráfego para o dispositivo AERSS.

DESTAQUES DE SEGURANÇA AERRSS

O dispositivo AERSS também possui recursos de segurança integrados, incluindo:

- Atualizações – Todos os softwares no AERSS são gerenciados na nuvem e atualizados com frequência para garantir que permaneçam atualizados e seguros. Isso inclui firmware, sistemas operacionais, aplicativos e patches.
- Certificados – O appliance AERSS usa certificados para proteger as configurações aplicadas à plataforma.
- Chaves de API – Os dados de log processados pela plataforma são autenticados no ActiveEye usando chaves de API dedicadas que são alternadas periodicamente para aumentar a segurança.
- Proteção da plataforma – A plataforma básica do appliance AERSS executa um sistema operacional reforçado.
- Monitoramento da plataforma – os logs do dispositivo AERSS são incluídos no monitoramento do ambiente.
- Comunicação – AERSS utiliza criptografia para todos os dados em trânsito. Todas as comunicações do appliance AERSS empregam criptografia para garantir que os dados confidenciais sejam protegidos contra possíveis espionagens.

CENTRO DE OPERAÇÕES DE SEGURANÇA

O Centro de Operações de Segurança ("Security Operations Center" - SOC) da Motorola Solutions pode monitorar redes, aplicativos e dispositivos contra ameaças de segurança 24 horas por dia, 7 dias por semana, via ActiveEye. Nossos analistas de SOC possuem habilidades técnicas profundas tanto no lado ofensivo quanto no defensivo da segurança. Com base em sua ampla experiência em segurança, nossos analistas de SOC recomendam configurações de dispositivos de segurança que otimizam a detecção de ameaças e implementam manuais para eliminar o ruído e abordar rapidamente as ameaças mais críticas. Isso coloca nosso foco na identificação de atividades que possam ser um risco ou incidente de segurança em potencial.

O SOC usa a capacidade do ActiveEye de priorizar alertas na fila e se concentrar em alertas com maior probabilidade de resultar em um incidente ou risco de segurança. A equipe de gerenciamento do SOC monitora regularmente os SLAs internos e estabeleceu KPIs internos para garantir que os alertas sejam investigados em tempo hábil.

Nosso SOC trabalha regularmente com novos clientes que estão em processo de mitigação e recuperação de um comprometimento. Usando ferramentas de EDR, a equipe detecta, investiga e interrompe ativamente os agentes de ameaças e seus ataques. Quando uma atividade suspeita é identificada, a equipe tem experiência para mitigar e interceptar rapidamente as ameaças antes da exploração ativa.

Se uma investigação de ameaça exigir a entrada de sua equipe de segurança, o SOC criará um caso de segurança e seguirá os procedimentos de escalonamento predefinidos para cada nível de prioridade. Se o SOC não puder alcançar o contato de primeiro nível, o SOC escalará de acordo com os procedimentos definidos pelo cliente. O ActiveEye permite que você visualize casos de segurança e histórico de investigação de eventos a qualquer momento. O SOC está sempre disponível para fornecer consultas adicionais sobre um Caso de Segurança, revisar os detalhes do Caso em profundidade ou fornecer assistência adicional com a investigação, conforme necessário.

No caso de um possível incidente, o SOC usará os dados disponíveis no ActiveEye e acessará seu sistema para determinar a extensão da atividade maliciosa. Se necessário, o SOC adicionará mais políticas de detecção aos seus módulos de serviço. Com o módulo de serviço EDR, o SOC pode realizar ações de mitigação em sistemas hosts remotos com base em um plano de resposta pré-aprovado ou se determinar que é necessário para um caso específico. Quando necessário, o SOC recomendará ações de mitigação que você pode tomar para lidar com uma ameaça.

Com investigação e resposta de segurança, o tempo é essencial. A maioria dos comprometimentos iniciais resultam em movimento lateral se não detectados e mitigados em 60 minutos. O SOC monitora de perto o tempo de resolução de seus alertas de segurança como uma medida conjunta de nossa capacidade de interagir e responder a atividades em seu ambiente. Essas métricas e tendências de tempo de resposta estão disponíveis em seu painel ActiveEye e em seus relatórios mensais.

Os analistas realizam treinamentos regulares sobre gerenciamento de dados de clientes e privacidade para proteger dados confidenciais de clientes.

A equipe do SOC participa rotineiramente de exercícios da equipe vermelha e da equipe roxa e processa plataformas de treinamento sofisticadas para garantir que suas habilidades estejam atualizadas. Nossos analistas seniores desenvolvem e executam exercícios do mundo real que simulam a atividade moderna de agentes de ameaças e violações de segurança para treinamento de analistas SOC.

ActiveEye pelos números: detectando e prevenindo malware*

2,078
amostras exclusivas de malware
RASTREADAS

RESULTING IN

6,392
AÇÕES DE RESPOSTA
implementadas

ALLOWING FOR

658,199
processos
IMPEDIDOS DE EXECUTAR

O que vou ver em um alerta do SOC?

- O que encontramos
- Nomes de analistas
- Quando encontramos
- Onde encontramos
- O que fizemos
- Resposta recomendada
- Detalhes técnicos

*Dados de 2021

Insights expandidos e planejamento estratégico de segurança

Revisão Mensal e Recomendações do Programa de Segurança

Análise de tendências e caça à ameaças

Pesquisas na Deep e Dark Webs

Analista de segurança nomeado

INSIGHTS AVANÇADOS DE AMEAÇAS

O ActiveEye Advanced Threat Insights é um serviço opcional que expande os serviços de monitoramento SOC padrão fornecidos pelo ActiveEye MDR. Esse serviço fornece uma função de pesquisa de segurança mais proativa e aprofundada para enriquecer a conscientização sobre sua postura de segurança cibernética em andamento, otimizar o valor dos controles de segurança existentes e, por fim, reduzir o risco de segurança cibernética.

Com o serviço Advanced Threat Insights, a Motorola Solutions designará um analista de segurança cibernética dedicado para trabalhar proativamente com você e sua equipe. O analista liderará um programa avançado de caça a ameaças para identificar ameaças avançadas específicas e resumir os padrões de ameaças em evolução de interesse. O analista designado usará o ActiveEye MDR e as ferramentas conectadas para pesquisar dados de log de segurança de endpoint, rede e nuvem em busca de evidências de comprometimentos não detectados na rede. Com base na inteligência de ameaças externas relevantes ou entidades de alto risco (contas de usuários ou sistemas) identificadas no ActiveEye ou por sua equipe, o analista designado pesquisará externamente nas contas de usuários corporativos de superfície, profundos e comprometidos, endereços IP corporativos conectados a botnets e dados para venda.

A cada mês, o analista designado se reunirá com sua equipe de segurança para fornecer uma visão geral de todas as ameaças detectadas no mês anterior e discutir a estratégia de segurança daqui para frente. Eles também compartilharão um relatório resumido dos resultados de busca de ameaças concluídos e mitigação sugerida e ameaças descobertas.

Embora o serviço Advanced Threat Insights ofereça inteligência profunda da superfície, profunda e escura. Como tal, não podemos garantir que possamos descobrir todas as ameaças em tempo real, pois alguns fóruns e comunidades clandestinas podem levar meses para aparecer ou para que pesquisadores de segurança obtenham acesso. Além disso, o escopo desses serviços não inclui serviços de investigação relacionados a funcionários, como aqueles que podem visar funcionários específicos (ou outros indivíduos) ou implicar direitos de privacidade, conduta interna alegada ou suspeita ou direitos que possam ser protegidos ou regulamentados por lei.

UMA PARCEIRA PARA SUAS NECESSIDADES DE CIBERSEGURANÇA

ESCALA GLOBAL E EXPERIÊNCIA

Com mais de 90 anos de experiência no gerenciamento de tecnologias de missão crítica e mais de 20 anos no desenvolvimento de soluções de segurança cibernética, a Motorola Solutions está bem posicionada para ser o "provedor de serviços único" para suas necessidades de segurança cibernética.

Com as melhores pessoas, processos e operações escaláveis de tecnologia que podem ajudar as organizações a gerenciar a conscientização, detecção, resposta e recuperação de riscos cibernéticos. Nossa plataforma de orquestração e automação de segurança de ponta, ActiveEye, oferece insights 24 horas por dia, 7 dias por semana, sobre possíveis ameaças ao seu ambiente e uma abordagem cogerenciada para o gerenciamento de segurança. Fornecemos uma abordagem desenvolvida e integrada para a resiliência cibernética de ponta a ponta.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com