Aranda Security Compliance

Saiba mais sobre as versões mais recentes do Aranda Security Compliance (ASEC)

Aqui você pode encontrar informações sobre atualizações nas funcionalidades do ASEC.

Nota da versão 9.5.0

Problema ao preencher o valor "Versão mínima" na política

PM-76959-19-202072

No ASEC, ao inserir uma política com critérios mínimos de verificação de versão, como no caso da navegação na web com o Microsoft Edge; Quando você define um valor para a versão mínima, salva, sai da política e entra novamente, o valor não é preservado.

Uma configuração é implementada para garantir que o valor mínimo da versão seja salvo corretamente após sair e entrar novamente na política.

Informações da loja

CHG-68809-19-301763

- Data das vulnerabilidades recentes

A funcionalidade é implementada para capturar e registrar as datas de criação e atualização de vulnerabilidades mais recentes. Isso permite maior precisão e rastreabilidade das informações, garantindo que os dados reflitam com precisão o estado atual das vulnerabilidades detectadas.

Graças a essa melhoria, as informações necessárias para a geração do Relatório de vulnerabilidade descoberto recentemente, que fornece uma lista detalhada de vulnerabilidades identificadas dentro de um período parametrizável. Este relatório facilita a análise de risco, a tomada de decisões estratégicas de segurança e o planejamento oportuno de ações corretivas.

Além disso, com o registro atualizado das datas de criação e modificação, o monitoramento das vulnerabilidades ao longo do tempo é otimizado, permitindo avaliar tendências, medir a eficácia das ações de mitigação e garantir uma gestão mais eficiente da segurança nos sistemas.

- Histórico de conformidade de um grupo

A funcionalidade é implementada para registrar e gerenciar o histórico de conformidade dos grupos associados às políticas. Isso permite que os níveis de conformidade sejam armazenados e rastreados ao longo do tempo, fornecendo informações detalhadas sobre sua evolução.

Graças a essa implementação, será possível gerar o Relatório de Conformidade, que fornecerá uma visão abrangente do status de cada grupo em relação às políticas estabelecidas, facilitando a análise, auditoria e tomada de decisões estratégicas.

- Usuário que executou a correção

O registro do usuário que executa a correção é implementado nos detalhes do dispositivo. Essa funcionalidade permite uma melhor rastreabilidade das ações tomadas, proporcionando maior visibilidade de quem executou cada correção e em que momento.

Graças a esse registro, é mais fácil rastrear as intervenções realizadas nos dispositivos, o que contribui para uma melhor gestão da auditoria e permite que decisões informadas sejam tomadas com base no histórico de ações. Isso ajuda a fortalecer o controle e a segurança nos processos de correção.

Atualização automática de metadados

- É implementada uma funcionalidade que permite a atualização automática do Metadados por Sistema Operacional. Esse processo cuida do carregamento, processamento e atualização de informações no banco de dados, garantindo que os dados reflitam com precisão o estado mais recente de cada sistema operacional.

Com essa melhoria, a gestão do Metadados, garantindo que quaisquer alterações ou novas informações relacionadas aos sistemas operacionais sejam processadas de forma eficiente e sem intervenção manual. Isso não apenas melhora a integridade e a consistência dos dados, mas também facilita a disponibilização para análise, relatórios e auditoria.

Além disso, ao automatizar esse processo, o risco de erro humano é reduzido, a eficiência operacional é aprimorada e as tarefas de manutenção e atualização de informações são simplificadas, fornecendo um banco de dados mais confiável e atualizado para a tomada de decisões estratégicas.

Nova funcionalidade de atividade de correção

- A Atividade de Correção, como parte dos detalhes de Dispositivos, apresenta o histórico de atividades de correção geradas por problemas de segurança descobertos.

Para obter mais detalhes, consulte a seguinte documentação:

- Atividade de correção ↪

Nova funcionalidade: exportar vulnerabilidades e dispositivos da lista

CHG-66794-19-301717

- A ação de Exportar a lista de vulnerabilidades e dispositivos detectados possibilita análises e auditorias de segurança, além de facilitar a organização e o monitoramento da infraestrutura tecnológica. A exportação de listas de vulnerabilidades e dispositivos pode ser gerada em formatos compatíveis, como CSV ou Excel, melhorando a eficiência no gerenciamento e relatório de dados críticos.

Para obter mais detalhes, consulte a seguinte documentação:

- Exportar lista de vulnerabilidades ↪
- Exportar lista ↪ de dispositivos

Políticas de filtro aprimoradas

- O filtro de política avançado é implementado com opções para realizar consultas por sistema operacional e associando dispositivos a políticas.

Para obter mais detalhes, consulte a seguinte documentação:

- Filtro de ↪ política

Notas ou instruções adicionais

- A atualização automática do agente requer os serviços do comum.

- O ASEC é lançado com a versão comum 9.9.1.6
- ASEC lançado com a versão 9.5.48 do banco de dados

⚠ Importante: Em instalações conjuntas entre produtos Aranda, você deve ter a mesma compatibilidade que a versão Common.

Nota da versão 9.4.2

Nova funcionalidade de exclusão de dispositivo

CHG-66615-19-301711

- A nova funcionalidade de remoção de dispositivos permite que os usuários gerenciem e limpem seu inventário com mais rapidez e eficiência. Agora é possível selecionar e remover vários dispositivos simultaneamente, simplificando o processo e economizando tempo. Além disso, esse recurso inclui a opção de desinstalar o agente do computador na mesma etapa, garantindo uma remoção completa do sistema. Isso é especialmente útil para manter um ambiente atualizado sem agentes desatualizados ou não autorizados nos dispositivos.

Melhora os detalhes da vulnerabilidade

CHG-65315-19-301690

- Cada vulnerabilidade fornece detalhes mais completos e acessíveis sobre cada ameaça detectada. Inclui campos claros para a descrição da vulnerabilidade e do software afetado, facilitando a compreensão do escopo de cada risco. Além disso, fornece referências a avisos, soluções e ferramentas recomendadas para mitigar a vulnerabilidade. Um filtro adicional permite exibir os dispositivos específicos que contêm essa vulnerabilidade, juntamente com a data de publicação e a última atualização. Esses detalhes atualizados ajudam a priorizar a resposta a cada vulnerabilidade com base na criticidade e relevância atuais.

Notas ou instruções adicionais

- A atualização automática do agente requer os serviços do comum.

- O ASEC é lançado com a versão comum 9.9.1.6
- O ASEC é lançado com a versão 9.5.47 do banco de dados

⚠ Importante: Em instalações conjuntas entre produtos Aranda, você deve ter a mesma compatibilidade que a versão Common.

Falha ao associar dispositivos a um grupo de processamento de pedidos

PM-73597-19-201986

Foi identificado um erro no console do ASEC, no módulo de grupos de conformidade, onde não era possível associar dispositivos aos grupos correspondentes. Como resultado, não foi realizada uma atribuição correta de dispositivos, afetando o gerenciamento e a conformidade das políticas no sistema.

É implementado um ajuste que permite que os dispositivos sejam adicionados com sucesso aos grupos de conformidade, garantindo um gerenciamento mais eficiente e alinhado aos requisitos da plataforma.

Nota de lançamento 9.4.1

Lista de dispositivos aprimorada

- Na lista, os ícones foram redesenhados para identificar dispositivos que não foram verificados e aqueles que não apresentam vulnerabilidades. Essas categorias são adicionadas aos filtros para melhorar a classificação.

Aprimoramento do agente

- Uma versão do agente é gerada para otimizar o desempenho nos dispositivos.

Notas ou instruções adicionais

- A atualização automática do agente requer os serviços do comum.

- O ASEC é lançado com a versão comum 9.9.0.11
- ASEC lançado com a versão 9.5.46 do banco de dados

⚠ Importante: Em instalações conjuntas entre produtos Aranda, você deve ter a mesma compatibilidade que a versão Common.

Nota de versão 9.4.0

Nova funcionalidade de vulnerabilidades

CHG-49175-19-301403

- A nova funcionalidade de detecção de vulnerabilidades permite identificar e gerenciar proativamente possíveis ameaças à segurança. Com esse sistema, o agente relata a varredura do dispositivo a cada 24 horas, detectando vulnerabilidades conhecidas por seu respectivo CVE. Isso torna mais fácil para os administradores de TI tomar medidas preventivas para proteger os dados e manter a integridade dos sistemas. Essa ferramenta é essencial para fortalecer a segurança cibernética e reduzir o risco de ataques.

Resumo da melhoria do módulo

CHG-52915-19-301494

- O módulo Resumo foi aprimorado para que clicar em qualquer um dos três painéis: "Conformidade da política por dispositivo", "Agentes instalados" e "Status da política" exiba informações mais detalhadas. Isso para facilitar o acesso e o gerenciamento dessas informações.

Notas ou instruções adicionais

- A atualização automática do agente requer os serviços do comum.

- O ASEC é lançado com a versão comum 9.9.0.11
- O ASEC é lançado com a versão 9.5.45 do banco de dados

⚠ Importante: Em instalações conjuntas entre produtos Aranda, você deve ter a mesma compatibilidade que a versão Common.

Nota da versão 9.3.0

Melhoria do módulo de licenciamento

CHG-53037-19-301517

- O módulo de licenciamento é ajustado para mostrar apenas a opção de usuários simultâneos na coluna "Usuários", porque não se aplica a usuários nomeados.

Módulo de gerenciamento de políticas aprimorado

CHG-53038-19-301518

- O módulo "Grupos de políticas" no menu "Configurações" é renomeado para "Grupos de conformidade" para dar mais contexto às funcionalidades da seção, pois aqui os dispositivos são agrupados para associá-los às políticas.

Configurar: validação de política para macOS e Linux

CHG-49172-19-301402

Para esta versão, foram feitos os seguintes ajustes:

- Esta versão configura o console para executar validações de política nos sistemas operacionais macOS e Linux.
- As versões do Agente são criadas para macOS e Linux.

Notas ou instruções adicionais

- A atualização automática do agente requer os serviços do comum.

- O ASEC é lançado com a versão comum 9.8.1.2
- ASEC lançado com a versão 9.5.43 do banco de dados

⚠ Importante: Em instalações conjuntas entre produtos Aranda, você deve ter a mesma compatibilidade que a versão Common.