A3A®
Engenharia
de Sistemas

Endpoint Hardening e Hardening de Sistemas

Solution Overview

2026

www.a3aengenharia.com.br

VISÃO GERAL

VISÃO GERAL

Endpoint Hardening é a aplicação estruturada de configurações, restrições e controles destinados a reduzir a superfície de ataque de sistemas e dispositivos. A solução da A3A Engenharia abrange estações de trabalho, servidores, aplicações, equipamentos de rede, plataformas de segurança eletrônica, dispositivos industriais e outros ativos conectados que precisam operar com uma configuração segura, documentada e compatível com sua função.

O trabalho não consiste em aplicar uma lista genérica de recomendações. Cada baseline precisa considerar sistema operacional, versão, função, criticidade, integrações, requisitos de disponibilidade, orientação do fabricante, políticas internas e limitações operacionais. Um controle adequado para uma estação administrativa pode ser incompatível com um servidor SCADA, uma câmera IP, um switch industrial ou uma estação de engenharia.

A A3A estrutura o hardening como um processo de engenharia: inventaria e classifica os ativos, identifica configurações inseguras, define a condição desejada, testa os controles em ambiente representativo, implementa as alterações de forma controlada, registra exceções e comprova o resultado por meio de evidências.

POR QUE CONFIGURAÇÕES PADRÃO NÃO SÃO SUFICIENTES

Sistemas operacionais, aplicações e equipamentos costumam ser entregues com recursos habilitados para facilitar instalação, compatibilidade e suporte a diferentes cenários. Essa flexibilidade pode manter contas, serviços, portas, protocolos, interfaces administrativas, permissões e componentes que não são necessários no ambiente real.

O hardening reduz essa exposição sem comprometer a operação. Serviços desnecessários são removidos ou desativados, privilégios são limitados, interfaces são protegidas, políticas são centralizadas e eventos relevantes passam a ser registrados. O objetivo é dificultar acesso inicial, escalonamento de privilégios, movimentação lateral, persistência e exfiltração.

COMO UMA CONSULTORIA DE HARDENING PODE AJUDAR

Uma consultoria especializada evita dois extremos: manter configurações frágeis por receio de impacto ou aplicar controles excessivamente restritivos sem compreender as dependências. A A3A transforma requisitos de segurança em parâmetros verificáveis, relacionando cada controle ao risco mitigado, ao ativo afetado, ao método de implantação e ao teste de validação.

Essa abordagem também permite separar correções imediatas de um programa de evolução. Credenciais padrão, serviços expostos e sistemas fora de suporte podem exigir tratamento prioritário, enquanto padronização, automação e monitoramento de conformidade podem ser implementados em ondas sucessivas.

Seu ambiente possui sistemas críticos, equipamentos legados ou configurações sem baseline formal?

A A3A pode realizar uma avaliação inicial, identificar os principais riscos de configuração e estruturar um plano de hardening compatível com a operação.

Solicitar avaliação técnica de hardening

OBJETIVOS

REDUZIR A SUPERFÍCIE DE ATAQUE

O primeiro objetivo é eliminar ou restringir componentes que não são necessários para a função do ativo. Isso envolve contas, serviços, aplicações, portas, interfaces, protocolos, extensões, scripts, recursos de administração e permissões excessivas.

PADRONIZAR CONFIGURAÇÕES SEGURAS

Uma baseline transforma recomendações dispersas em uma configuração aprovada, controlada por versão e aplicável a uma classe de ativos. A padronização reduz diferenças injustificadas entre equipamentos e facilita implantação, auditoria, suporte e recuperação.

PROTEGER IDENTIDADES E PRIVILÉGIOS

O hardening deve limitar contas administrativas, remover credenciais padrão, aplicar menor privilégio, separar funções, proteger contas de serviço e restringir a administração a origens autorizadas. Quando aplicável, a arquitetura pode ser integrada a MFA, PAM, RADIUS, TACACS+, certificados e diretórios corporativos.

AUMENTAR CAPACIDADE DE DETECÇÃO E RESPOSTA

Uma configuração segura também precisa produzir evidências. Logs de autenticação, processos, alterações, falhas, serviços, aplicações e produtos de segurança devem ser coletados e protegidos. A integração com SIEM e ferramentas de monitoramento permite detectar desvios e investigar incidentes.

PRESERVAR DISPONIBILIDADE E SUPORTABILIDADE

Segurança não pode ser aplicada de forma desconectada da continuidade. A baseline precisa respeitar aplicações críticas, contratos de suporte, recomendações do fabricante, janelas de manutenção, procedimentos de rollback e requisitos de recuperação. Controles incompatíveis devem ser tratados como exceções formais, com medidas compensatórias e prazo de revisão.

ESCOPO DE ATUAÇÃO

INVENTÁRIO, CLASSIFICAÇÃO E DIAGNÓSTICO

O trabalho começa pela identificação dos ativos realmente abrangidos. São levantados função, proprietário, localização, sistema operacional, firmware, aplicações, interfaces, dependências, exposição, criticidade e condição de suporte. O diagnóstico compara a configuração atual com a condição segura definida para cada classe.

A análise pode combinar documentação, coleta de configurações, entrevistas, inspeção técnica e ferramentas automatizadas. O resultado diferencia vulnerabilidade de software, falha de configuração, ausência de governança, obsolescência e exposição arquitetural.

DESENVOLVIMENTO DA BASELINE DE SEGURANÇA

A baseline é construída a partir de requisitos do cliente, guias do fabricante, CIS Benchmarks, NIST, ASD Information Security Manual e referências específicas da tecnologia. As recomendações são adaptadas ao contexto; não são copiadas integralmente sem avaliação de impacto.

Cada item deve indicar parâmetro esperado, justificativa, método de aplicação, forma de verificação, criticidade e tratamento de exceção. A baseline recebe identificação de versão e passa a integrar o processo de gestão de mudanças.

HARDENING DE ESTAÇÕES DE TRABALHO

Estações corporativas, administrativas e de engenharia podem receber políticas para contas locais, privilégios, Secure Boot, proteção contra exploits, firewall local, dispositivos removíveis, aplicações autorizadas, macros, navegadores, scripts, PowerShell, atualizações, criptografia, bloqueio de tela e telemetria de segurança.

A configuração pode ser distribuída por GPO, MDM, ferramentas de gestão, scripts ou mecanismos equivalentes. Antes da implantação ampla, é recomendável validar perfis representativos de usuários e aplicações.

HARDENING DE SERVIDORES E SERVIÇOS CRÍTICOS

Servidores exigem baselines específicas por função. Controladores de domínio, servidores de certificados, bancos de dados, aplicações web, hipervisores, servidores SCADA, VMS, sistemas de monitoramento e plataformas de gestão possuem requisitos diferentes.

O escopo pode abranger contas de serviço, privilégios, serviços ativos, protocolos, firewall, criptografia, permissões de arquivos, interfaces administrativas, backups, logs, aplicações instaladas e separação de funções. Servidores críticos devem evitar funções adicionais que ampliem desnecessariamente a superfície de ataque.

ACTIVE DIRECTORY, IDENTIDADE E CONTAS PRIVILEGIADAS

Ambientes baseados em Active Directory podem exigir revisão de controladores de domínio, GPOs, trusts, delegações, contas administrativas, contas de serviço, políticas de autenticação, LDAP, Kerberos e acesso aos backups. Contas de alto privilégio devem ser separadas das contas de uso cotidiano.

A solução pode ser integrada a PAM e jump server, MFA e políticas de acesso privilegiado. O objetivo é reduzir exposição de credenciais e melhorar rastreabilidade.

HARDENING DE APLICAÇÕES

O sistema operacional pode estar protegido enquanto aplicações permanecem com módulos, contas, APIs, extensões, serviços e permissões inseguros. O hardening deve abranger aplicações de usuário e de servidor, incluindo navegadores, suítes de escritório, leitores de PDF, bancos de dados, servidores web, middleware e plataformas de gestão.

Também podem ser definidos controles de execução de aplicações, bibliotecas, scripts, instaladores e drivers. Eventos de bloqueio e permissão devem ser registrados para ajuste da política e investigação.

SWITCHES, ROTEADORES, FIREWALLS E APPLIANCES

Hardening de infraestrutura de rede inclui AAA, SSH, certificados, SNMPv3, syslog, NTP, ACLs de gerenciamento, serviços desnecessários, proteção de portas, spanning tree, backups, firmware e ciclo de vida. A configuração deve respeitar a função de cada equipamento e a topologia.

Em ambientes Cisco, o hardening de switches Cisco pode ser integrado a Cisco ISE, RADIUS, TACACS+, 802.1X e políticas de segmentação. Em redes industriais, controles de camada 2 precisam ser avaliados para não comprometer protocolos e redundância.

CÂMERAS IP, NVR, VMS E CONTROLE DE ACESSO

Dispositivos de segurança eletrônica frequentemente permanecem conectados por longos ciclos de vida e podem possuir serviços, contas e interfaces administrativas expostos. O

hardening pode abranger câmeras, gravadores, servidores VMS, controladoras, terminais, integrações e estações de operação.

São avaliados firmware, credenciais, certificados, protocolos, acesso remoto, segmentação, APIs, logs, sincronismo, armazenamento e comunicação com serviços externos. Guias de fabricantes, como Axis, Milestone e demais plataformas utilizadas, são incorporados à baseline do projeto.

SISTEMAS INDUSTRIAIS E AMBIENTES OT

Servidores SCADA, estações de engenharia, IHMs, gateways, RTUs, IEDs, CLPs e appliances industriais exigem análise específica. Atualizações ou bloqueios podem impactar disponibilidade, certificações, suporte do fabricante e segurança do processo.

A implantação em OT deve considerar homologação, janela, backup, imagem do sistema, rollback, redundância, comunicação com fornecedores e medidas compensatórias. Quando o ativo não suporta o controle desejado, segmentação, monitoramento, jump server, firewall e restrição de acesso podem reduzir o risco.

ATUALIZAÇÕES, FIRMWARE E GESTÃO DE VULNERABILIDADES

Hardening não substitui gestão de vulnerabilidades e atualizações. A A3A pode apoiar identificação de versões, análise de suporte, priorização, homologação, implantação e validação de patches e firmware.

Nem toda correção pode ser aplicada imediatamente. Exceções devem registrar risco, justificativa, proteção compensatória, responsável e prazo de reavaliação. Equipamentos sem suporte precisam integrar um plano de modernização.

EDR, FIREWALL LOCAL E CONTROLE DE APLICAÇÕES

O hardening pode incluir integração com EDR/XDR, antivírus, firewall local, controle de dispositivos e application control. Esses produtos precisam ser configurados conforme criticidade e comportamento normal do sistema.

Políticas muito permissivas reduzem proteção; políticas aplicadas sem teste podem bloquear aplicações legítimas. A implantação deve utilizar modo de auditoria, piloto, ajuste e expansão controlada quando a tecnologia permitir.

LOGS, MONITORAMENTO E INTEGRAÇÃO COM SIEM

São definidos eventos prioritários, retenção, sincronismo, origem e destino dos logs. Autenticações, alterações de política, criação de processos, falhas, serviços, aplicativos, produtos de segurança e ações administrativas podem ser encaminhados a coletores e SIEM.

A coleta precisa ser dimensionada e testada. Logs sem horário confiável, contexto do ativo ou retenção adequada têm valor limitado para auditoria e resposta a incidentes.

PILOTO, IMPLANTAÇÃO CONTROLADA E ROLLBACK

A baseline é validada em ativos representativos antes da expansão. O piloto verifica aplicações, desempenho, administração, atualizações, integrações, logs e procedimentos operacionais. Problemas identificados são tratados antes de atingir sistemas de maior criticidade.

A implantação pode ocorrer por grupos, sites ou classes de equipamentos. Cada mudança deve possuir pré-requisitos, backup, critérios de go/no-go, teste pós-alteração e rollback.

Hardening exige configuração, integração e validação coordenadas.

A A3A pode apoiar a implementação das baselines em sistemas, equipamentos e plataformas, preservando rastreabilidade entre requisito, mudança e evidência.

Conhecer o serviço de Parametrização e Configuração de Sistemas

ENTREGÁVEIS

Os entregáveis dependem da etapa contratada, da quantidade de tecnologias e do nível de implementação. O pacote técnico pode reunir diagnóstico, definição da baseline, plano de implantação e evidências de conformidade.

DIAGNÓSTICO E PLANEJAMENTO

BASELINE E DOCUMENTAÇÃO DE CONFIGURAÇÃO

IMPLANTAÇÃO E EVIDÊNCIAS

GOVERNANÇA E MANUTENÇÃO

MODELO DE CONTRATAÇÃO

ASSESSMENT INDEPENDENTE

Indicado para organizações que precisam conhecer o estado atual, priorizar riscos e definir um programa de hardening antes de implementar mudanças. O assessment pode abranger uma tecnologia, um site ou um conjunto de ativos críticos.

DESENVOLVIMENTO DE BASELINE

A A3A pode elaborar baselines e critérios de conformidade para implementação pela equipe interna, por um fornecedor ou por um integrador. O escopo inclui análise de impacto, exceções e roteiro de validação.

IMPLEMENTAÇÃO E REMEDIAÇÃO

O trabalho pode avançar para piloto, parametrização, aplicação das configurações, atualização, integração com ferramentas e validação. Responsabilidades, acessos, janelas e contingências são definidos antes da intervenção.

OWNER'S ENGINEERING E FISCALIZAÇÃO TÉCNICA

A A3A pode atuar como engenharia do proprietário, revisando baselines, planos de mudança, evidências, exceções e documentação produzida por fabricantes, integradores ou equipes contratadas.

SERVIÇO CONTINUADO DE CONFORMIDADE

Ambientes que mudam continuamente podem exigir revisão periódica de configuração, acompanhamento de vulnerabilidades, atualização de baselines, verificação de desvios e apoio a novas tecnologias. O escopo pode ser estruturado como serviço continuado de engenharia consultiva.

COMISSIONAMENTO E ACEITE

Quando o hardening integra um projeto ou implantação maior, o aceite pode verificar aderência à baseline, funcionamento das aplicações, acesso administrativo, logs, contingência, rollback e comportamento dos produtos de segurança.

APLICABILIDADE

AMBIENTES CORPORATIVOS E DATA CENTERS

Estações, notebooks, servidores, Active Directory, virtualização, bancos de dados, aplicações corporativas, equipamentos de rede e plataformas de administração podem ser organizados em baselines por função e criticidade.

INDÚSTRIAS, UTILITIES E INFRAESTRUTURAS CRÍTICAS

Ambientes OT exigem hardening compatível com disponibilidade, segurança do processo, suporte do fabricante e janelas restritas. A atuação pode abranger centros de operação, subestações, plantas industriais, mineração, saneamento, energia, logística e instalações distribuídas.

SEGURANÇA ELETRÔNICA E SISTEMAS IP

Câmeras, NVRs, VMS, controle de acesso, interfonia, analíticos, servidores e estações de operação podem ser protegidos por baseline específica, segmentação, gestão de credenciais, atualização, certificados e monitoramento.

PROJETOS DE MODERNIZAÇÃO E ADEQUAÇÃO

O hardening pode integrar projetos de telecomunicações, redes Cisco, modernização de servidores, implantação de EDR/XDR, SIEM, Cisco ISE, segmentação, Zero Trust e atualização de sistemas legados.

POR QUE A A3A ENGENHARIA

A A3A reúne competências em cibersegurança, redes, telecomunicações, automação, segurança eletrônica, integração e comissionamento. Essa visão multidisciplinar permite avaliar o hardening no contexto da arquitetura e da operação, evitando configurações isoladas que criem incompatibilidades ou riscos de disponibilidade.

A atuação pode começar por um diagnóstico específico e evoluir para baseline, implantação, integração com ferramentas, Owner’s Engineering ou conformidade contínua. O escopo é definido conforme criticidade, quantidade de ativos, diversidade tecnológica e nível de intervenção necessário.

Precisa estruturar ou revisar o hardening de sistemas críticos?

Informe as tecnologias, quantidade aproximada de ativos, principais riscos, restrições de mudança e objetivo da contratação para que a Engenharia da A3A avalie o melhor modelo de atendimento.

Apresentar a demanda à Engenharia da A3A

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas