A3A®
Engenharia
de Sistemas

SIEM para Gestão de Eventos e Monitoramento de Segurança

Solution Overview

2026

www.a3aengenharia.com.br

VISÃO GERAL

VISÃO GERAL

A solução de **Security Information and Event Management (SIEM)** da A3A Engenharia de Sistemas é direcionada a organizações que precisam centralizar registros, aumentar a visibilidade sobre eventos de segurança, estruturar casos de uso de detecção e fornecer evidências confiáveis para investigação e resposta a incidentes. A atuação pode abranger diagnóstico, arquitetura, dimensionamento, especificação, implantação, integração, desenvolvimento de detecções, validação e evolução da plataforma.

Um SIEM recebe eventos de diferentes fontes, normaliza e enriquece os dados, relaciona atividades e apresenta alertas, pesquisas, painéis e trilhas de auditoria. Sua utilidade, porém, não depende apenas da tecnologia escolhida. Fontes incompletas, logs sem sincronismo, campos mal interpretados, regras genéricas e ausência de processo operacional podem transformar a plataforma em um repositório caro, com muitos eventos e pouca capacidade de detecção.

A A3A posiciona o SIEM dentro de uma arquitetura integrada de cibersegurança. A plataforma deve conversar com EDR/XDR, Endpoint Hardening, identidade, firewalls, redes, aplicações, sistemas industriais, ferramentas de monitoramento e processos de resposta. O objetivo é transformar dados técnicos em sinais acionáveis, não apenas concentrar mensagens de syslog.

SIEM NÃO É APENAS ARMAZENAMENTO DE LOGS

Centralizar logs é uma etapa necessária, mas não suficiente. Uma arquitetura madura define quais eventos são relevantes, por quanto tempo devem ser retidos, quais campos precisam estar disponíveis, como o horário será sincronizado, como a integridade será preservada e quais perguntas a equipe precisa responder durante uma investigação.

A partir dessa base, casos de uso relacionam eventos de autenticação, endpoint, rede, nuvem, aplicações e sistemas críticos. Um alerta relevante pode depender de várias evidências: autenticação anômala, elevação de privilégio, execução suspeita, alteração de configuração e comunicação com destino incomum. Sem contexto e qualidade de dados, a correlação perde valor.

COMO UMA CONSULTORIA DE SIEM PODE AJUDAR

A consultoria transforma uma intenção ampla de “implantar SIEM” em requisitos técnicos e operacionais verificáveis. A A3A identifica ativos e fontes prioritárias, avalia formatos e volumes, define arquitetura, retenção, acesso, casos de uso, integrações, responsabilidades, critérios de aceite e plano de evolução.

Esse trabalho reduz riscos comuns: licenciamento subdimensionado, ingestão indiscriminada, perda de eventos importantes, retenção incompatível com a investigação, regras sem contexto, excesso de falsos positivos e dependência de conhecimento não documentado. Também permite avaliar plataformas e propostas a partir de critérios comuns, e não somente de demonstrações comerciais.

Sua organização precisa estruturar, revisar ou ampliar uma plataforma SIEM?

A A3A pode realizar um diagnóstico das fontes, volumes, casos de uso, integrações e processos atuais para definir uma arquitetura compatível com o risco e a capacidade operacional.

Solicitar assessment técnico de SIEM

OBJETIVOS

CENTRALIZAR REGISTROS RELEVANTES E PRESERVAR EVIDÊNCIAS

O SIEM deve consolidar eventos necessários para segurança, auditoria e investigação, preservando origem, data, usuário, endereços, ação, resultado e demais atributos úteis. A coleta precisa ser acompanhada por controles de integridade, sincronismo de horário, disponibilidade e capacidade de armazenamento.

DETECTAR ATIVIDADES SUSPEITAS COM CONTEXTO

O objetivo não é alertar sobre cada evento isolado, mas identificar combinações, sequências e desvios relevantes. Casos de uso podem relacionar autenticação, privilégios, alterações de configuração, atividade de endpoint, acesso remoto, tráfego, DNS, nuvem e aplicações.

APOIAR TRIAGEM, INVESTIGAÇÃO E RESPOSTA

A plataforma precisa reduzir o tempo necessário para compreender o que ocorreu, quais ativos e usuários foram afetados, qual foi a sequência dos eventos e quais ações devem ser tomadas. Pesquisas, linhas do tempo, enriquecimento e integração com tickets ou playbooks apoiam esse processo.

AUMENTAR RASTREABILIDADE E GOVERNANÇA

Trilhas de auditoria, relatórios e controles de acesso ajudam a demonstrar quem realizou determinada ação, quando ela ocorreu e como o evento foi tratado. O SIEM também pode apoiar verificações internas, requisitos contratuais e processos de conformidade, sem substituir a governança necessária para interpretar e responder aos dados.

CONTROLAR VOLUME, CUSTO E QUALIDADE DOS DADOS

Mais dados não significam necessariamente mais segurança. O projeto deve equilibrar cobertura, detalhamento, retenção, desempenho e custo. Eventos duplicados, mensagens sem utilidade e campos incompletos consomem capacidade sem melhorar a investigação.

ESCOPO DE ATUAÇÃO

INVENTÁRIO DE ATIVOS E FONTES DE EVENTOS

O trabalho começa pela identificação das fontes disponíveis e das lacunas de cobertura. São considerados firewalls, switches, roteadores, VPNs, diretórios, servidores, endpoints, aplicações, bancos de dados, DNS, proxies, e-mail, nuvem, sistemas de backup, plataformas de segurança e ativos operacionais.

Cada fonte é classificada por criticidade, finalidade, responsável, método de coleta, formato, volume, qualidade, frequência, retenção e casos de uso suportados. Essa matriz orienta prioridades e evita conectar fontes sem objetivo definido.

ASSESSMENT DA ARQUITETURA E OPERAÇÃO EXISTENTES

Quando já existe SIEM ou centralização de logs, a A3A pode avaliar cobertura, coletores, filas, parsers, normalização, retenção, capacidade, regras, dashboards, acessos, integrações e rotinas operacionais. O diagnóstico identifica eventos perdidos, fontes silenciosas, saturação, duplicidade, erros de parsing, regras sem proprietário e alertas não tratados.

ARQUITETURA CENTRALIZADA, DISTRIBUÍDA, CLOUD OU HÍBRIDA

A arquitetura pode utilizar coletores locais, concentradores por unidade, filas, armazenamento em camadas e processamento centralizado ou distribuído. A decisão depende de volume, latência, conectividade, soberania dos dados, criticidade, disponibilidade, operação e custo.

Ambientes com múltiplos sites ou redes segregadas podem exigir coletores intermediários, buffers locais e mecanismos de recuperação após falhas de comunicação. Em OT, a coleta deve respeitar zonas, conduítes, DMZ industrial e restrições de tráfego entre redes.

DIMENSIONAMENTO DE INGESTÃO, CAPACIDADE E RETENÇÃO

O dimensionamento considera eventos por segundo, picos, tamanho médio, crescimento, compressão, indexação, replicação, consultas, dashboards e retenção. O projeto pode separar armazenamento de alta performance para investigação recente e camadas de menor custo para retenção prolongada.

A política de retenção precisa considerar necessidade de investigação, requisitos internos, obrigações aplicáveis, sensibilidade e custo. Um prazo único para todas as fontes normalmente é ineficiente; eventos críticos e trilhas administrativas podem exigir tratamento diferente de logs operacionais de baixo valor.

COLETA POR SYSLOG, AGENTES, APIS E INTEGRAÇÕES NATIVAS

A coleta pode utilizar syslog, Windows Event Forwarding, agentes, conectores, APIs, filas, bancos de dados e serviços de nuvem. O método deve preservar disponibilidade, segurança, autenticação, criptografia e capacidade de recuperação.

Também são definidos tratamento de falhas, monitoramento dos coletores, armazenamento temporário, rotação, certificados e responsáveis. A ausência de alertas sobre uma fonte que deixou de enviar eventos é uma falha de segurança e de observabilidade da própria plataforma.

SINCRONISMO DE HORÁRIO E INTEGRIDADE DA LINHA DO TEMPO

Correlação e investigação dependem de relógios consistentes. O projeto deve definir fontes NTP confiáveis, hierarquia de sincronismo, timezone, tratamento de equipamentos legados e verificações de desvio. Sem isso, eventos relacionados podem aparecer em ordem incorreta ou inviabilizar uma reconstrução confiável.

PARSING, NORMALIZAÇÃO E QUALIDADE DOS DADOS

Mensagens recebidas precisam ser interpretadas de maneira consistente. Parsing extrai campos; normalização traduz formatos distintos para um modelo comum; enriquecimento acrescenta contexto de ativos, identidades, criticidade, localização e inteligência de ameaças.

A qualidade é validada por amostragem e testes. Um evento recebido, mas com usuário, endereço, resultado ou ação interpretados incorretamente, pode gerar correlação errada. Mudanças de versão e firmware também podem alterar formatos e exigir manutenção dos parsers.

CASOS DE USO E ENGENHARIA DE DETECÇÃO

Casos de uso são priorizados conforme riscos, ativos críticos, histórico e capacidade de resposta. Exemplos incluem tentativas de acesso anômalas, criação de contas privilegiadas, alteração de políticas, desativação de controles, execução suspeita, movimentação lateral, acesso remoto incomum, varreduras, exfiltração e atividade em

horários ou locais incompatíveis.

Quando aplicável, os casos podem ser relacionados a táticas e técnicas do MITRE ATT&CK. Cada detecção deve possuir objetivo, fontes necessárias, lógica, severidade, condições de exclusão, responsável, procedimento de triagem, teste e periodicidade de revisão.

CORRELAÇÃO, ANALYTICS E REDUÇÃO DE FALSOS POSITIVOS

As regras podem combinar eventos, janelas de tempo, frequência, contexto de ativo, identidade e comportamento histórico. A correlação deve aumentar o valor do sinal, não apenas multiplicar alertas.

O tuning analisa falsos positivos, exceções legítimas, limiares e dados ausentes. Ajustes precisam ser documentados para evitar que a redução de ruído elimine visibilidade sobre comportamentos relevantes.

INTEGRAÇÃO COM EDR/XDR, IDENTIDADE, FIREWALLS E NAC

O SIEM pode relacionar telemetria de endpoint, autenticação, privilégios, tráfego, e-mail, nuvem e rede. EDR/XDR fornece contexto de processos e resposta; diretórios e IAM identificam usuários e grupos; firewalls e NAC contribuem com sessões, acessos e ações de contenção.

A Integração de Sistemas documenta protocolos, APIs, certificados, campos, severidades, filas, limites, tratamento de falha e responsabilidade por cada interface. O projeto evita encaminhar toda a telemetria sem avaliar utilidade, volume e custo.

DASHBOARDS, RELATÓRIOS E INDICADORES

Painéis devem responder perguntas operacionais: fontes ativas, saúde da coleta, alertas abertos, ativos afetados, principais técnicas observadas, tendências, cobertura e tempo de tratamento. Dashboards executivos e técnicos possuem objetivos diferentes e não devem depender da mesma granularidade.

TRIAGEM, PLAYBOOKS E INTEGRAÇÃO COM RESPOSTA

Alertas precisam estar associados a procedimentos. Playbooks podem definir validação, coleta de contexto, classificação, escalonamento, contenção, preservação de evidências, comunicação e encerramento. Integrações com service desk ou SOAR podem automatizar tarefas repetitivas, desde que os limites e níveis de autorização estejam definidos.

SIEM EM REDES INDUSTRIAIS E AMBIENTES OT

Em ambientes industriais, o SIEM pode receber eventos de firewalls, switches, servidores SCADA, historians, estações de engenharia, máquinas de salto, diretórios, sistemas de acesso remoto e plataformas de visibilidade OT. A coleta deve respeitar arquitetura, disponibilidade, protocolos e restrições operacionais.

O artigo técnico sobre SIEM em ambientes OT e subestações aprofunda fontes, casos de uso e particularidades desses ambientes. Informações de Cisco Cyber Vision e outras plataformas de inventário podem enriquecer o contexto dos eventos.

PRIVACIDADE, SEGREGAÇÃO E ACESSO AOS DADOS

Logs podem conter identificadores, endereços, comandos, ações de usuários e outros dados sensíveis. O projeto define perfis de acesso, segregação de funções, mascaramento quando aplicável, auditoria administrativa, retenção e descarte. O SIEM não deve se tornar um repositório sem governança.

TESTES, TUNING E COMISSIONAMENTO

O aceite deve comprovar que as fontes enviam os eventos previstos, campos são interpretados corretamente, regras geram alertas esperados, dashboards apresentam dados consistentes e falhas de coleta são detectadas. Testes controlados validam cenários sem colocar o ambiente em risco.

O valor do SIEM depende da qualidade das integrações e dos casos de uso.

A A3A integra fontes corporativas, redes, endpoints, identidade, segurança eletrônica e ambientes OT com critérios de capacidade, segurança, rastreabilidade e aceite.

Conhecer o serviço de Integração de Sistemas

ENTREGÁVEIS

DIAGNÓSTICO E PLANEJAMENTO

ARQUITETURA E INTEGRAÇÃO

CASOS DE USO E OPERAÇÃO

TESTES E DOCUMENTAÇÃO

MODELO DE CONTRATAÇÃO

ASSESSMENT DE LOGS E MATURIDADE

Indicado para organizações que desejam compreender fontes disponíveis, lacunas, volumes, qualidade, retenção, regras e capacidade operacional antes de adquirir ou ampliar uma plataforma.

PROJETO E ESPECIFICAÇÃO INDEPENDENTE

A A3A pode desenvolver arquitetura, requisitos, dimensionamento, critérios de seleção, prova de conceito e aceite antes da contratação da tecnologia. Esse modelo permite comparar propostas com base em objetivos e requisitos comuns.

IMPLANTAÇÃO E INTEGRAÇÃO

O escopo pode incluir plataforma, coletores, fontes, parsers, regras, dashboards, integrações, testes e documentação. Responsabilidades sobre licenças, infraestrutura, suporte e operação são definidas contratualmente.

OWNER'S ENGINEERING E FISCALIZAÇÃO TÉCNICA

A A3A pode representar o contratante durante aquisição e implantação executadas por fabricantes, integradores ou prestadores de serviço, revisando arquitetura, capacidade, casos de uso, testes, evidências e documentação.

ENGENHARIA CONTINUADA DE DETECÇÃO

Após a implantação, serviços continuados podem abranger inclusão de fontes, manutenção de parsers, desenvolvimento e revisão de casos de uso, tuning, análise de cobertura, indicadores e melhoria dos playbooks.

Esse modelo não equivale automaticamente a SOC ou MDR 24x7. Monitoramento permanente, triagem contínua, plantão, tempos de resposta e autoridade para contenção precisam de escopo, equipe e níveis de serviço específicos.

COMISSIONAMENTO E ACEITE TÉCNICO

O serviço de Comissionamento e Aceite Técnico verifica cobertura, capacidade, parsing, correlação, alertas, integrações, acessos, retenção, dashboards e documentação.

APLICABILIDADE

AMBIENTES CORPORATIVOS E HÍBRIDOS

Aplicável a organizações com usuários, endpoints, servidores, aplicações locais, serviços de nuvem, VPNs, filiais e múltiplas ferramentas de segurança que precisam de visibilidade e investigação centralizadas.

DATA CENTERS E WORKLOADS CRÍTICOS

Atende ambientes com virtualização, bancos de dados, identidade, backup, aplicações críticas e infraestrutura de rede, nos quais alterações, acessos e indisponibilidades precisam de rastreabilidade.

INDÚSTRIAS, UTILITIES E INFRAESTRUTURAS CRÍTICAS

Em OT, a solução pode integrar eventos de redes industriais, servidores SCADA, estações de engenharia, máquinas de salto, firewalls, acesso remoto, plataformas de inventário e sistemas de automação, respeitando arquitetura e continuidade operacional.

SEGURANÇA ELETRÔNICA E SISTEMAS IP

Logs de VMS, NVRs, câmeras, controle de acesso, servidores e plataformas de gestão podem contribuir para auditoria, detecção de falhas, alterações administrativas e investigação, desde que a integração seja suportada e tecnicamente justificada.

ORGANIZAÇÕES COM REQUISITOS DE AUDITORIA E MÚLTIPLOS SITES

SIEM é especialmente útil quando existem diferentes unidades, equipes, fornecedores, aplicações e controles, e a organização precisa consolidar evidências, padronizar visibilidade e acompanhar eventos de forma coordenada.

POR QUE A A3A ENGENHARIA

A A3A integra competências de cibersegurança, redes, telecomunicações, sistemas industriais, segurança eletrônica, hardening, EDR/XDR, integração e comissionamento. Essa visão multidisciplinar permite identificar fontes e casos de uso além do perímetro tradicional de TI.

A abordagem privilegia requisitos, capacidade, qualidade de dados, documentação, implantação por fases e critérios objetivos de aceite. O objetivo é entregar uma plataforma

que sustente investigação e governança, evitando um ambiente com grande volume de logs, alto custo e baixa utilização operacional.

Um projeto de SIEM deve começar pelos riscos, fontes e casos de uso — não pela quantidade de dados que a plataforma consegue ingerir.

Informe ambiente, quantidade de sites, ferramentas atuais, fontes prioritárias, requisitos de retenção e modelo operacional esperado. A Engenharia da A3A pode estruturar o escopo adequado.

Apresentar a demanda de SIEM 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