xFabric
Unified Security Fabric Platform

WHITE PAPER TÉCNICO

Unified Security Fabric

Arquitetura de referência para um plano de controle único em ambiente multicloud

Modelo de dados comum, chave estável de ativo, correlação por grafo e retenção em camadas com residência por jurisdição. Inclui matriz de decisão entre consolidação e integração e critérios de aceite mensuráveis.

Documento técnico xFabric · revisão 2026.2 · uso corporativo

Contexto e fundamentação

A justaposição de consoles produz correlação probabilística e custo operacional permanente. Um plano de controle único normaliza telemetria em modelo de dados comum e transforma detecção em decisão auditável.

O custo estrutural da justaposição de consoles

A maioria das operações de segurança em ambiente multicloud opera entre seis e doze consoles independentes. Cada console mantém seu próprio identificador de ativo, sua própria janela de retenção e seu próprio vocabulário de severidade. A consequência não é apenas ergonômica: a correlação entre domínios passa a depender de heurística de nome de host, endereço IP efêmero ou carimbo de tempo aproximado.

Em termos operacionais, isso significa que o tempo médio de investigação cresce proporcionalmente ao número de fontes, não ao número de eventos. O analista gasta a maior parte do intervalo entre detecção e contenção reconstruindo contexto que já existia na origem e foi perdido na fronteira entre ferramentas.

Modelo de dados comum como pré-requisito

Consolidação começa na ingestão. Cada evento — chamada de API de nuvem, telemetria de endpoint, log de identidade, achado de postura — é normalizado para um esquema único de entidade, ação, sujeito e recurso, com chave estável de ativo derivada da própria fonte autoritativa do provedor.

Com chave estável, a correlação deixa de ser probabilística. Uma credencial comprometida no provedor de identidade, uma chamada anômala de API e um processo suspeito no host convergem para o mesmo objeto de investigação porque referenciam o mesmo identificador, não porque coincidem no tempo.

- Chave de ativo derivada do inventário do provedor, não de hostname
- Severidade calculada por impacto no negócio, não herdada da fonte
- Linhagem completa do evento preservada para cadeia de custódia
- Retenção em camadas com trilha imutável para evidência regulatória

Correlação determinística e supressão de ruído

Sobre um modelo de dados comum, a correlação passa a operar por grafo: identidade, workload, rede e dado formam um caminho de exposição verificável. O grafo permite responder à pergunta que importa — se esta credencial for usada, o que ela alcança — antes de o incidente ocorrer.

O efeito prático mais relevante é a supressão de falso positivo com justificativa. Um achado de postura em um bucket sem exposição de rede e sem princípio externo autorizado é rebaixado por evidência estrutural, não por regra de silenciamento manual que envelhece sem revisão.

Critérios de aceite para uma consolidação

Uma migração para plano de controle unificado deve ser medida antes e depois com os mesmos indicadores. Sem linha de base, a consolidação vira narrativa.

- Cobertura ATT&CK; por tática, medida por detecção validada em exercício
- Tempo médio entre detecção e contenção por classe de incidente
- Percentual de achados com dono nomeado e prazo de remediação
- Custo por gigabyte retido por camada e por jurisdição de residência
- Percentual de alertas fechados por automação com revisão amostral

Matriz de decisão: consolidação ou integração

A decisão entre consolidar em um plano de controle único e integrar ferramentas existentes deve ser tomada por critério verificável, e não por inércia contratual. A matriz abaixo compara as duas abordagens nos eixos que determinam custo total de operação.

Eixo	Integração de consoles	Plano de controle único
Chave de correlação	Heurística de host, IP e tempo	Identificador estável do inventário do provedor
Severidade	Herdada de cada fonte	Calculada por impacto no negócio
Retenção	Janela distinta por ferramenta	Camadas com política única e trilha imutável
Evidência	Exportação manual por console	Cadeia de custódia contínua
Custo marginal por fonte	Conector, tradução e manutenção	Normalização no ingest
Automação	Por ferramenta, escopo limitado	Playbook único sobre grafo completo

Arquitetura de referência

Camada de coleta

Agente de endpoint, conectores de API de nuvem, ingestão de syslog e integrações de identidade escrevem em um barramento único. Cada evento carrega origem, jurisdição de coleta e carimbo confiável antes de qualquer transformação.

Camada de normalização

Decodificação, enriquecimento com inventário autoritativo e atribuição da chave estável de ativo. Eventos sem chave resolvível são retidos em quarentena para reconciliação, nunca descartados silenciosamente.

Camada de análise

Regras determinísticas, correlação por grafo e modelos de priorização operam sobre o mesmo modelo de dados. O resultado é um caso com linha do tempo, ativos envolvidos, técnica ATT&CK; mapeada e ação recomendada.

Camada de resposta e governança

Playbooks com escopo declarado, RBAC multi-tenant, residência de dados por região e API de exportação para ITSM e SOAR do cliente.

Critérios de aceite e plano de medição

Os indicadores a seguir devem ser coletados antes do início da migração e recoletados ao final de cada fase. A ausência de linha de base invalida a comparação.

Indicador	Unidade	Critério de aceite
Cobertura ATT&CK; validada	% de técnicas priorizadas	Aumento frente à linha de base, verificado em exercício
Tempo até contenção	minutos, por classe	Redução sustentada em três ciclos consecutivos
Achados com dono e prazo	% do total aberto	Acima do limite acordado no plano de remediação
Custo por GB retido	moeda / GB / camada	Igual ou inferior ao modelo anterior
Alertas fechados por automação	% com revisão amostral	Precisão medida acima do limite de promoção

Checklist de implantação

- Inventário autoritativo por provedor conectado e reconciliado
- Definição da chave estável de ativo e política de quarentena
- Mapa de jurisdições de residência e política de retenção por camada
- Modelo de RBAC e segregação multi-tenant aprovado
- Linha de base dos cinco indicadores de aceite registrada
- Exercício adversário inicial executado e lacunas priorizadas
- Integração com ITSM e trilha de auditoria validada ponta a ponta

Pontos de decisão

- Integração preserva o custo de tradução entre ferramentas; consolidação o elimina na ingestão.
- Sem chave estável de ativo, toda correlação entre domínios permanece probabilística.
- Consolidação sem linha de base medida não é verificável — defina indicadores antes da migração.