VAI NA WEB
CURSO DE CIBERSEGURANÇA

Proposta Técnica - LojaZeta

Versão:1.0

Karyne Guinyver Dias da Silva

Brasília
19/09/2025

1. SUMÁRIO EXECUTIVO

A LojaZeta, um e-commerce em fase de crescimento, opera em infraestrutura de nuvem com tecnologia baseada em Nginx, Node.js e PostgreSQL. Apesar do avanço no mercado digital, a empresa vem enfrentando ameaças recorrentes de SQL Injection (SQLi), Cross-Site Scripting (XSS) e ataques de força bruta em endpoints críticos, como o /login. Esses incidentes refletem a necessidade de reforçar a proteção das aplicações e dos dados sensíveis de clientes, que são o principal ativo do negócio.

O ambiente atual apresenta vulnerabilidades estruturais, como a ausência de um SIEM consolidado para correlação e análise de eventos, a dispersão de logs entre diferentes instâncias e a falta de testes de restauração de backups, o que representa um risco significativo de perda de disponibilidade e confiabilidade em caso de incidente grave. Além disso, o time interno é enxuto, composto por apenas dois desenvolvedores e um profissional de operações, o que exige uma estratégia de segurança que seja pragmática, escalável e alinhada às restrições de orçamento.

Para enfrentar esses desafios, propõe-se a implementação de uma arquitetura de defesa em camadas, que contempla proteção no perímetro, rede, host, aplicação, dados e identidade, com foco na mitigação imediata das ameaças mais críticas. Paralelamente, recomenda-se a criação de um monitoramento centralizado mínimo viável (MVP de SIEM), permitindo consolidar logs essenciais, gerar alertas acionáveis e oferecer visibilidade ao time de operações.

O plano também inclui a adoção de um processo simplificado de resposta a incidentes (IR) baseado no framework NIST IR, estruturado nas fases de detecção, contenção, erradicação, recuperação e lições aprendidas. Além disso, serão desenvolvidos runbooks objetivos para os principais cenários enfrentados pela LojaZeta: tentativas de SQLi, XSS, brute-force e indisponibilidade de serviço.

Os ganhos esperados com a adoção deste plano são claros:Redução do risco de indisponibilidade por incidentes de segurança.Maior visibilidade e controle sobre ataques em andamento, através de alertas centralizados.Melhoria nos tempos médios de detecção (MTTD) e resposta (MTTR), aumentando a resiliência operacional.

Confiança ampliada para clientes e stakeholders, demonstrando compromisso com segurança e continuidade.Com essa abordagem 80/20, priorizando quick wins nos primeiros 30 dias, a LojaZeta estará preparada para elevar significativamente seu nível de maturidade em segurança, sem comprometer a agilidade e o orçamento do negócio.

2. ESCOPO E METODOLOGIA

O escopo desta proposta concentra-se em três pilares fundamentais: a segurança das aplicações web utilizadas pela LojaZeta, a proteção da identidade dos usuários e do time interno, e a segurança dos dados críticos, especialmente informações de clientes e transações financeiras. Além disso, está incluída a implementação de um monitoramento centralizado mínimo viável, que permita consolidar logs e gerar alertas acionáveis. Também

faz parte do escopo o desenvolvimento de runbooks básicos de resposta a incidentes, oferecendo orientações claras e rápidas para lidar com os cenários mais prováveis, como tentativas de SQLi, XSS, ataques de força bruta e indisponibilidade do serviço.

Alguns pontos estão fora do escopo imediato devido a limitações de orçamento e equipe. Entre eles estão a implementação de um SOC 24/7, a realização de testes avançados de Red Team e a adoção de um SIEM corporativo completo, soluções que demandam recursos mais robustos e times maiores para operar de forma eficaz. Essas iniciativas podem ser consideradas em uma etapa futura, de médio a longo prazo, quando a maturidade em segurança da LojaZeta for maior.

A metodologia utilizada nesta consultoria baseia-se na análise do ambiente atual, considerando a pilha tecnológica (Nginx, Node.js, PostgreSQL) e os incidentes recentes reportados. A partir dessa análise, são aplicadas boas práticas de segurança defensiva (Blue Team), com foco no modelo de segurança em camadas e no ciclo de resposta a incidentes do NIST IR, que estrutura as etapas de detecção, contenção, erradicação, recuperação e lições aprendidas.

Algumas assunções foram consideradas para viabilizar a proposta: que a infraestrutura em nuvem no modelo IaaS permite flexibilidade para configuração de regras de rede, segmentação e controle de acessos; e que a equipe técnica possua pelo menos conhecimentos básicos de Linux e administração de sistemas, garantindo a execução prática das recomendações.

Em resumo, o escopo e a metodologia foram pensados de forma a entregar o máximo impacto em segurança com o mínimo de recursos, priorizando medidas de alto valor e rápida implementação, em linha com as necessidades e a realidade da LojaZeta.

3. ARQUITETURA DE DEFESA (CAMADAS)

A segurança da LojaZeta será estruturada em camadas complementares, seguindo o princípio de defesa em profundidade. Cada camada contribui para reduzir riscos e proteger os principais ativos do negócio.

Perímetro

No ponto de entrada da aplicação, será utilizado um WAF gerenciado (como Cloudflare ou NGINX com ModSecurity CRS) para filtrar ataques comuns, como SQL Injection e XSS, antes que cheguem ao servidor. Será aplicado rate limiting no endpoint /login, bloqueando tentativas automáticas de força bruta. Além disso, pode-se adicionar CAPTCHA em fluxos críticos, reduzindo o risco de acessos automatizados maliciosos.

Rede

A rede será segmentada, isolando o banco de dados em uma sub-rede privada, acessível apenas pela aplicação. As listas de controle de acesso (ACLs) serão configuradas de forma mínima, permitindo apenas o tráfego necessário. Para acessos administrativos, será criado

um bastion host protegido com MFA, garantindo que qualquer acesso interno siga boas práticas de segurança.

Host

Os servidores que suportam a aplicação terão hardening baseado em guias como o CIS Benchmark, desabilitando serviços desnecessários e reforçando configurações padrão. As atualizações automáticas serão aplicadas para correções críticas de segurança, reduzindo a janela de exposição. Também será configurado o Fail2ban para bloquear tentativas de login SSH suspeitas.

Aplicação

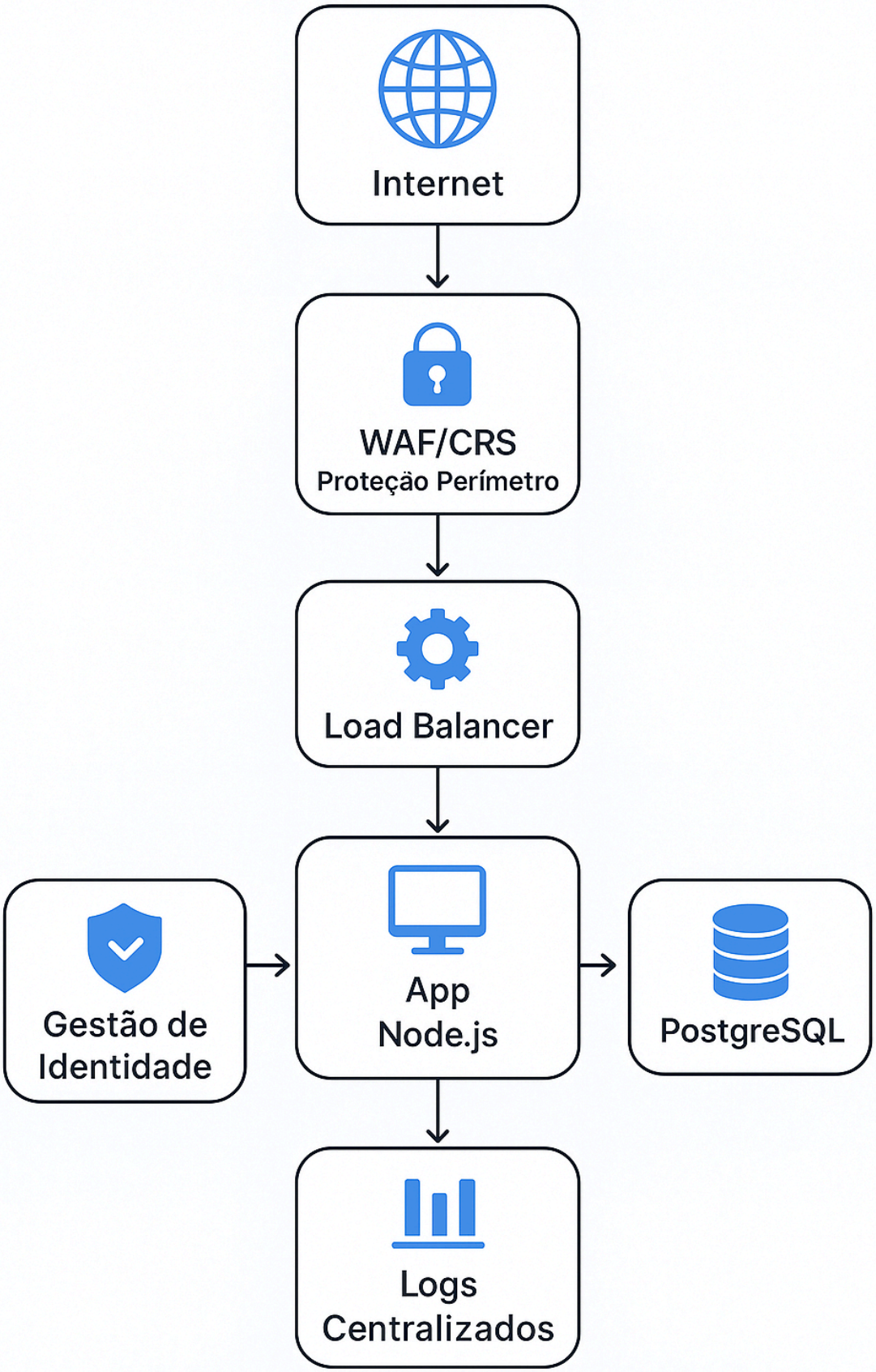
A aplicação Node.js passará a adotar validação e sanitização de entradas em todas as requisições, reduzindo a chance de SQLi e XSS. O uso de ORM seguro será incentivado para evitar queries manuais inseguras. O painel administrativo receberá proteção extra com MFA, garantindo que apenas usuários autorizados possam acessá-lo.

Dados

Todos os dados serão protegidos em trânsito, com uso obrigatório de TLS/HTTPS, e em repouso, por meio de criptografia em disco e no banco de dados. Os backups também serão criptografados e armazenados em local seguro. Além disso, serão realizados testes periódicos de restauração, assegurando que os backups possam ser recuperados com sucesso em caso de incidente.

Identidade

O controle de identidade será fortalecido com a adoção de uma gestão centralizada de segredos, utilizando ferramentas como HashiCorp Vault ou Secret Manager para evitar que credenciais fiquem expostas em código ou servidores. Todas as permissões seguirão o princípio do menor privilégio, garantindo que cada usuário ou serviço só tenha acesso ao que realmente precisa.


Internet
WAF/CRS
Proteção Perímetro
Load Balancer
Gestão de Identidade
App Node.js
PostgreSQL
Logs Centralizados

4. MONITORAMENTO & SIEM

O sistema coleta logs de Nginx, Node.js, PostgreSQL, Sistema Operacional e WAF.Todos os registros são centralizados no Loki, que exibe os dados no Grafana.Se precisar de algo mais avançado, pode ser evoluído para ELK Stack.

Com esses logs, o sistema gera alertas automáticos quando:

Há várias tentativas de login falhas em pouco tempo.O WAF detecta ataques como SQL Injection ou XSS.O aplicativo gera erros críticos.Um backup falha na restauração.

Além disso, são acompanhadas métricas importantes:MTTD: tempo médio para detectar um incidente.MTTR: tempo médio para corrigir o problema.Número de ataques bloqueados pelo WAF.Percentual de logs integrados no sistema.

5. RESPOSTA A INCIDENTES

1. Detecção

O incidente pode ser identificado por meio dos alertas do WAF ou do SIEM, além de dashboards de segurança que mostram atividades suspeitas ou falhas críticas.

2. Contenção

Após confirmar o incidente, a prioridade é reduzir o impacto. Isso pode incluir isolar a instância afetada, bloquear endereços IP maliciosos e revogar credenciais comprometidas.

3. Erradicação

Nesta etapa, é feita a remoção da causa do problema. Pode envolver corrigir vulnerabilidades, aplicar atualizações de segurança (patching) ou ajustar as regras de firewall e do WAF.

4. Recuperação

Uma vez corrigido o problema, os serviços devem ser restaurados com base em backups já testados, garantindo integridade e disponibilidade. Durante esse processo, é essencial monitorar o tráfego para identificar possíveis novos sinais de ataque.

5. Lições Aprendidas

Até cinco dias após o incidente, deve ser feito um post-mortem documentando o que aconteceu, quais medidas funcionaram e o que pode ser melhorado no futuro.

Runbooks (mínimo viável)

SQL Injection (SQLi): bloquear o IP atacante, revisar os logs de consultas, aplicar correções no ORM e reforçar medidas de hardening.

Cross-Site Scripting (XSS):
identificar o payload usado, reforçar a validação de entradas no código e atualizar as regras do WAF.
Brute Force: ativar bloqueio temporário do usuário ou IP, ajustar limites de tentativas de login e forçar a redefinição de senhas.Indisponibilidade: acionar o procedimento de backup e restauração, comunicar o status da operação e monitorar a integridade do sistema após a recuperação.

6. RECOMENDAÇÕES

A estratégia de segurança segue o princípio 80/20, priorizando ações de alto impacto e rápida implementação, garantindo proteção eficiente mesmo com recursos limitados.

Quick Wins – 30 dias

Nas primeiras semanas, as ações de maior impacto e menor complexidade serão implementadas:
Ativar o WAF e configurar rate limiting no login, bloqueando ataques automatizados e brute-force.

Centralizar os logs das aplicações, banco de dados, sistema e WAF em Loki + Grafana, permitindo visibilidade rápida de incidentes.Executar teste de restauração de backup, garantindo que os dados possam ser recuperados com segurança em caso de falha.Criar runbooks mínimos para os cenários mais críticos, como ataques de brute-force e SQLi, garantindo resposta rápida da equipe.

Médio Prazo – 90 dias

Após a implementação dos quick wins, o foco será expandir a segurança:
Ativar MFA (autenticação multifator) para devs e ops, aumentando a proteção de contas críticas.

Implementar hardening automatizado dos hosts, garantindo que todas as máquinas sigam boas práticas de segurança de forma consistente.Configurar dashboards de segurança com KPIs para monitorar incidentes, MTTD, MTTR e cobertura de logs.Desenvolver playbooks expandidos, incluindo XSS e cenários de indisponibilidade, detalhando ações passo a passo para cada tipo de incidente.Longo Prazo – 180 dias

No período de seis meses, as ações focam em maturidade e resiliência:

Adotar gestão centralizada de segredos, usando ferramentas como Vault ou Secret Manager, evitando exposição de credenciais em código ou servidores.

Expandir o WAF com regras customizadas, refinando a proteção contra ameaças específicas ao ambiente da LojaZeta.
Realizar treinamento contínuo para devs e ops em IR, garantindo que toda a equipe saiba como reagir a incidentes de forma rápida e eficiente.

Responsáveis

Devs: segurança do código, uso correto de ORM, implementação de MFA e validação de entradas.Ops: hardening de hosts, centralização de logs, execução de backup/restore, monitoramento.Consultoria: apoio na configuração do SIEM, criação de runbooks e orientação de melhores práticas.Essa abordagem permite resultados rápidos e mensuráveis nos primeiros 30 dias, enquanto constrói bases sólidas para proteção contínua e escalável ao longo do ano.

7. RISCOS, CUSTOS E ASSUNÇÕES ,LIMITAÇÕES, DEPENDÊNCIAS, ORÇAMENTO DE FERRAMENTAS

Riscos

A implementação do plano de segurança enfrenta alguns desafios que precisam ser considerados:

- **Equipe pequena:** com apenas dois desenvolvedores e um profissional de operações, a capacidade de executar todas as recomendações simultaneamente é limitada. Por isso, é essencial priorizar **ações de maior impacto** e automatizar processos sempre que possível.

- **Orçamento restrito:** algumas soluções de segurança corporativas, como SIEM completo ou WAF avançado, podem ter custos elevados. A proposta prioriza ferramentas **open-source ou serviços gerenciados de baixo custo**, garantindo segurança dentro das limitações financeiras.

Custos

Para manter os custos controlados, recomenda-se:

- Utilização de **ferramentas open-source**, como **Loki + Grafana** para centralização de logs e visualização de alertas, e **Fail2ban** para proteção básica de hosts.

- **Serviços gerenciados opcionais**, como **Cloudflare WAF**, que oferece proteção contra ataques comuns por um custo baixo (~$20/mês).

- O investimento é direcionado principalmente para soluções que entreguem **rápido retorno em segurança** e facilitem a operação da equipe enxuta.

Assunções

A proposta considera algumas premissas essenciais para que a estratégia funcione de forma prática:

- A infraestrutura em nuvem **IaaS** da LojaZeta permite integração com ferramentas de monitoramento e configuração de regras de rede.

- A equipe técnica possui **acesso root/admin** aos sistemas, garantindo que possa aplicar patches, hardening, MFA e alterações no WAF.

- O time tem **conhecimento básico de Linux e operação de sistemas**, permitindo operar os processos de segurança e responder a incidentes conforme os runbooks definidos.

8. CONCLUSÃO

A implementação das medidas propostas permitirá à LojaZeta aumentar significativamente sua resiliência frente a ameaças críticas, protegendo dados de clientes, aplicações e infraestrutura. As ações de curto prazo, baseadas no princípio 80/20, trazem resultados rápidos em 30 dias, focado em medidas de alto impacto e fácil execução, mesmo com equipe enxuta e orçamento limitado.

A evolução planejada para 90 e 180 dias garante uma maturidade gradual em segurança, incluindo: MFA para devs/ops, hardening automatizado de hosts, dashboards de monitoramento e gestão centralizada de segredos. Essa abordagem permite que a LojaZeta cresça com segurança, mantendo controle sobre incidentes e vulnerabilidades.

Próximos Passos:

Validar escopo com o time interno, garantindo alinhamento com prioridades e capacidade da equipe.Implementar quick wins identificados nos primeiros 30 dias, como WAF, rate limiting, centralização de logs e testes de backup.
Executar testes de resposta a incidentes (IR) usando os runbooks criados, certificando que os procedimentos funcionam e a equipe está preparada.Monitorar KPIs e métricas, ajustando processos conforme necessidade e garantindo melhoria contínua da segurança.

Critérios de Sucesso:

Redução de incidentes críticos, prevenindo impactos negativos nos serviços e na confiança dos clientes.100% de cobertura mínima dos logs, integrados ao SIEM ou ferramenta de monitoramento.Tempo de recuperação (MTTR) menor que 4 horas em casos de indisponibilidade, assegurando continuidade do serviço.

Execução efetiva dos runbooks nos incidentes simulados ou reais, garantindo que a equipe siga processos claros e padronizados.Com essa abordagem, a LojaZeta alcançará uma segurança prática, eficiente e escalável, alinhada à realidade da equipe e do orçamento, ao

mesmo tempo em que estabelece uma base sólida para crescimento seguro e sustentável do negócio.