

Escola Vai na Web

Trilha CyberSec

Módulo 2

# Consultoria

**Cliente:** LojaZeta

**Autor:** Emily Carla Fernandes

**Data:** 29 de setembro de 2025

**Versão:** 1.0

## Sumário

1. Sumário Executivo.....	3
2. Escopo e Metodologia .....	4
3. Arquitetura de Defesa .....	4
3.1 Diagrama da arquitetura de defesa em camadas .....	5
4. Monitoramento & SIEM .....	6
5. Resposta a Incidentes .....	6
6. Recomendações 80/20 e Roadmap (30/90/180 dias) .....	7
7. Riscos, Custos e Assunções .....	8
8. Conclusão .....	8

# 1. Sumário Executivo

Este documento apresenta uma proposta de estratégia de cibersegurança desenvolvida para a LojaZeta, com o objetivo de fortalecer sua infraestrutura tecnológica (Nginx, Node.js, PostgreSQL em IaaS) e estabelecer uma base resiliente para o crescimento do negócio, considerando as restrições de uma equipe enxuta e orçamento limitado.

A análise da postura de segurança atual revela uma tríade de riscos críticos que ameaçam a operação: a exposição a ataques web, evidenciada por tentativas recentes de SQL Injection e força bruta; a falta de visibilidade de segurança ("cegueira de segurança") devido à ausência de um sistema centralizado de logs (SIEM), o que impede a detecção de ameaças em tempo real; e o risco à continuidade do negócio, representado por uma política de backups que não inclui testes de restauração, tornando-os não confiáveis.

Para mitigar estes riscos, a solução proposta fundamenta-se em três pilares estratégicos: uma Arquitetura de Defesa em Profundidade, que cria barreiras de segurança sobrepostas; a implementação de Visibilidade e Detecção Centralizada através de uma plataforma SIEM *open-source* para monitoramento proativo; e a formalização de um plano de Resposta a Incidentes (IR), baseado no *framework* do NIST, para garantir uma reação rápida e coordenada durante uma crise. Este investimento, focado em soluções *open-source* de baixo custo, visa reduzir drasticamente a superfície de ataque, melhorar os tempos de detecção e resposta (MTTD/MTTR) e assegurar a resiliência operacional, transformando a segurança num pilar estratégico para o negócio.

## 2. Escopo e Metodologia

O escopo desta proposta abrange a arquitetura de segurança, a estratégia de monitoramento e o plano de resposta a incidentes para a plataforma de e-commerce da LojaZeta, focando-se nos ativos em produção no ambiente IaaS: servidores web, de aplicação e bases de dados. A segurança de TI corporativa e a segurança física estão fora do escopo. A metodologia de análise baseou-se nas informações fornecidas pelo cliente, em padrões da indústria como o NIST Cybersecurity Framework e o OWASP Top 10, e no princípio de Pareto (80/20), que prioriza a implementação dos controlos que mitigam a maior parte dos riscos mais críticos.

## 3. Arquitetura de Defesa

A estratégia de defesa adota a filosofia de Defesa em Profundidade, que pressupõe que nenhum controlo isolado é infalível, sendo necessária a implementação de múltiplas camadas de segurança sobrepostas.

A primeira camada, no perímetro, será um Web Application Firewall (WAF). Recomenda-se o OWASP Coraza WAF com o Core Rule Set (CRS), uma solução *open-source* de alta performance para proteger a aplicação contra ataques como SQLi e XSS. A sua implementação será faseada: primeiro em modo de monitoramento para analisar o tráfego e ajustar regras, evitando falsos positivos, e depois em modo de bloqueio para proteção ativa.

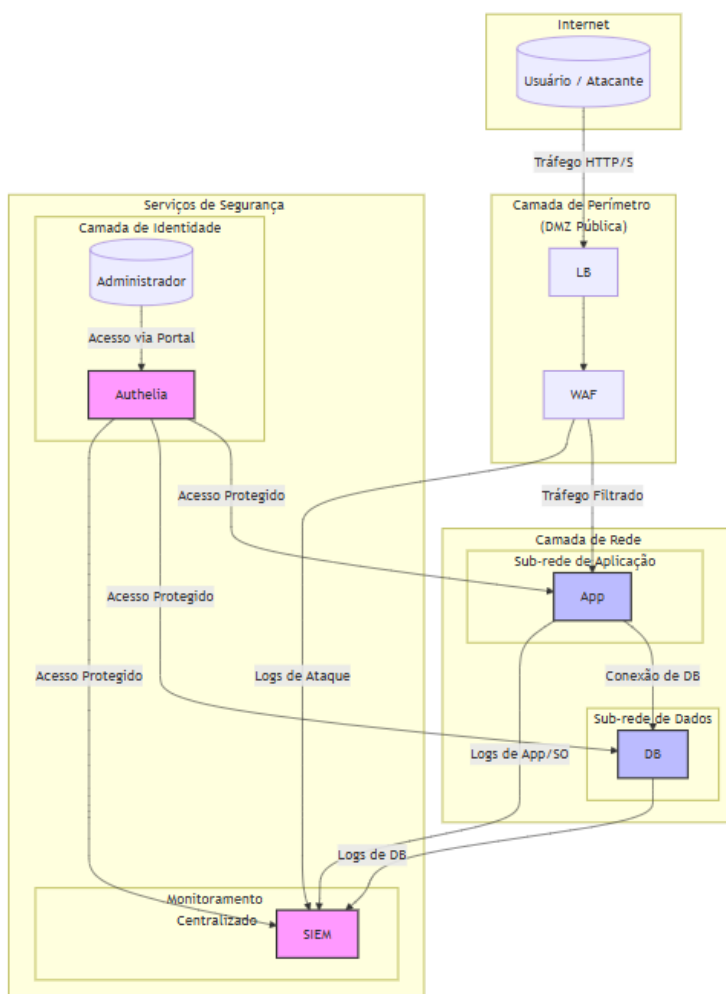
Na camada de rede, a estratégia é a segmentação. Utilizando os recursos nativos do provedor de nuvem (VPC, Sub-redes), a infraestrutura será dividida em zonas isoladas: uma sub-rede pública (DMZ) para o WAF e o *load balancer*, uma sub-rede de aplicação privada para os servidores Node.js e uma sub-rede de dados ainda mais restrita para o PostgreSQL. Esta arquitetura impede o movimento lateral de um atacante e aplica o princípio do privilégio mínimo, onde apenas as comunicações estritamente necessárias são permitidas.

O hardening de hosts e da aplicação constitui a terceira camada. Isto envolve fortalecer cada componente individualmente: usar sistemas operacionais "endurecidos", configurar *headers* de segurança no Nginx, e na aplicação Node.js, implementar análise de composição de software (SCA) com OSV-Scanner para detetar dependências vulneráveis, gerir segredos de forma segura fora do código, aplicar *rate limiting* para mitigar ataques de força bruta e introduzir testes dinâmicos de segurança (DAST) com OWASP ZAP.

Para a camada de dados, a proteção do PostgreSQL é crucial. Além do isolamento na rede, será implementado o arquivamento contínuo e a recuperação para um ponto no tempo (PITR), uma estratégia de backup muito superior à atual. Mais importante, será instituído um processo de teste de restauração trimestral obrigatório, a única forma de garantir que os backups são funcionais e que a equipe está preparada para uma recuperação de desastres.

Finalmente, na camada de identidade e acesso, o acesso administrativo será centralizado e fortalecido. A implementação do Authelia, um servidor de autenticação *open-source*, permitirá a criação de um portal de *Single Sign-On* (SSO) com a obrigatoriedade de Autenticação Multifator (MFA). Esta medida neutraliza eficazmente o risco de roubo de credenciais e acesso não autorizado a sistemas críticos.

### 3.1 Diagrama da arquitetura de defesa em camadas



## 4. Monitoramento & SIEM

Para resolver o problema da "cegueira de segurança", é essencial centralizar a visibilidade sobre os eventos da infraestrutura. A recomendação é a implementação do Wazuh, uma poderosa plataforma *open-source* que funciona como SIEM e XDR (Extended Detection and Response). O Wazuh não só agrega logs de múltiplas fontes (Nginx, Node.js, PostgreSQL, SO, WAF), mas também oferece detecção de intrusão baseada em host (HIDS) e monitoramento da integridade de ficheiros (FIM).

Com os logs centralizados, serão configuradas regras de correlação para detectar atividades maliciosas e gerar alertas acionáveis. Casos de uso prioritários incluem a deteção de tentativas de força bruta (múltiplas falhas de login), a identificação de ataques web a partir dos logs do WAF, e a deteção de atividades suspeitas como a criação de ficheiros executáveis nos diretórios da aplicação (um indicador de *web shell*). Para medir a eficácia desta implementação, serão acompanhados KPIs como o Tempo Médio para Detetar (MTTD) e o Tempo Médio para Responder (MTTR).

## 5. Resposta a Incidentes

Um plano de resposta a incidentes (IR) é fundamental para gerir crises de forma ordenada e minimizar danos. A LojaZeta adotará o ciclo de vida de resposta a incidentes do NIST SP 800-61, um padrão da indústria que estrutura a resposta em quatro fases: Preparação; Deteção e Análise; Contenção, Erradicação e Recuperação; e Atividade Pós-Incidente (lições aprendidas).

Será formalizada uma Equipe de Resposta a Incidentes de Segurança Cibernética (CSIRT), composta pela equipe técnica existente, com papéis e responsabilidades claramente definidos através de uma matriz RACI para eliminar a confusão durante um evento de alta pressão. Para garantir uma resposta consistente e eficaz, serão desenvolvidos runbooks — guias passo a passo para cenários de ameaça específicos. Por exemplo, um runbook para uma tentativa de Injeção de SQL detalharia os passos exatos para analisar o alerta, conter a ameaça (bloqueando o IP do atacante), erradicar a vulnerabilidade (corrigindo o código) e recuperar o sistema.

## 6. Recomendações 80/20 e Roadmap (30/90/180 dias)

Seguindo o princípio 80/20, o *roadmap* prioriza ações de alto impacto para obter ganhos de segurança rápidos e mensuráveis.

Fase	Período	Ações Prioritárias
<b>Fase 1: Visibilidade</b>	30 dias	<ul style="list-style-type: none"><li>- Implantar o WAF em modo de monitoramento para analisar o tráfego de ataques.</li><li>- Instalar o Wazuh para centralizar os primeiros logs (SO e Nginx).</li><li>- Fortalecer todas as senhas de acesso administrativo.</li></ul>
<b>Fase 2: Fortalecimento</b>	90 dias	<ul style="list-style-type: none"><li>- Ativar o WAF em modo de bloqueio.</li><li>- Implementar a segmentação de rede para conter ameaças.</li><li>- Integrar mais logs ao SIEM.</li><li>- Desenvolver e testar os primeiros runbooks de resposta a incidentes.</li></ul>
<b>Fase 3: Maturidade</b>	180 dias	<ul style="list-style-type: none"><li>- Implementar o Authelia com MFA para todo o acesso administrativo.</li><li>- Executar o primeiro teste obrigatório de restauração de backup.</li><li>- Introduzir caça a ameaças (threat hunting) com o Wazuh.</li><li>- Realizar testes de segurança dinâmicos (DAST) na aplicação.</li></ul>

## 7. Riscos, Custos e Assunções

A implementação desta estratégia acarreta alguns riscos, como a possibilidade de o WAF bloquear tráfego legítimo (falsos positivos) e a sobrecarga de alertas para a equipe. Estes riscos são mitigados pela implementação faseada do WAF e pelo ajuste fino das regras de alerta no SIEM. A principal restrição é a disponibilidade da equipe enxuta, que será gerida através do *roadmap* incremental e da automação que as ferramentas proporcionam.

Em termos de custos, a proposta foi desenhada para ser economicamente viável. O custo de *software* é zero, pois todas as ferramentas centrais recomendadas (Coraza, Wazuh, Authelia) são *open-source*. Os custos diretos são marginais, limitados aos recursos de nuvem adicionais para hospedar as novas ferramentas e armazenar logs. O principal investimento é o custo operacional, ou seja, o tempo da equipe dedicado à implementação e gestão. A proposta assume que a equipe possui a proficiência técnica necessária e que haverá comprometimento da liderança para a execução do plano.

## 8. Conclusão

A LojaZeta está num ponto de inflexão onde a sua postura de segurança reativa já não é sustentável. A estratégia aqui delineada move a empresa para um modelo proativo e resiliente, construindo uma base sólida para o crescimento futuro. O sucesso será medido por critérios claros, como a redução de 90% nos incidentes de ataques web, a melhoria dos KPIs de resposta a incidentes (MTTD < 1 hora, MTTR < 4 horas) e uma taxa de sucesso de 100% nos testes de restauração de *backup*.

Os próximos passos recomendados são agendar uma reunião de alinhamento para aprovação do plano, seguida de um *workshop* técnico para dar início à Fase 1 e estabelecer reuniões de acompanhamento quinzenais para monitorar o progresso.