VAI NA WEB – CYBERSEC

PROPOSTA – Opção 2 (Consultoria)

PAULO DOUGLAS WANDERLEY BEZERRA

JABOATÃO DOS GUARARAPES/PE, 20 DE SETEMBRO DE 2025

1. Sumário Executivo

A **LojaZeta**, um e-commerce em expansão, apresenta riscos de segurança típicos de ambientes expostos na internet:

- Tentativas recentes de **SQL Injection, XSS e brute-force em /login**.
- **Ausência de SIEM**, com logs descentralizados.
- **Backups feitos mas não testados**, comprometendo a confiabilidade.
- **Equipe pequena e orçamento limitado**, exigindo soluções simples e efetivas.

Visão da solução:

- Implantar **defesa em camadas** com foco em aplicação e identidade.
- Estabelecer um **monitoramento centralizado mínimo viável** (logs unificados + alertas acionáveis).
- Adotar um **plano de resposta a incidentes baseado no NIST IR**.

Ganhos esperados:

- Redução imediata do risco de exploração de falhas web.
- Aumento da visibilidade sobre incidentes.
- Capacidade de resposta estruturada e repetível.
- Evolução gradual da maturidade de segurança (80/20: esforço mínimo, maior impacto).

2. Escopo e Metodologia

Escopo:

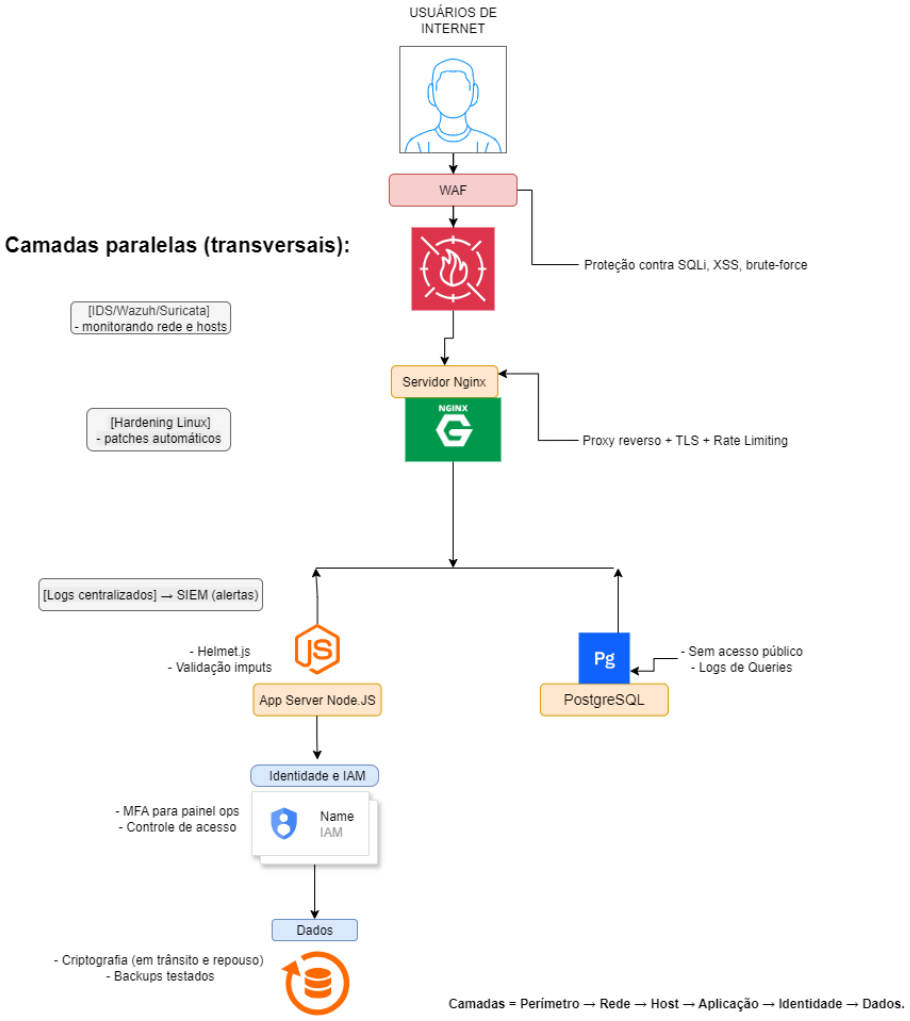
- Análise focada na stack atual (Nginx + Node.js + PostgreSQL) hospedada em IaaS.
- Considera apenas controles técnicos e operacionais aplicáveis ao cenário da LojaZeta.
- Ênfase em: segurança de aplicação, identidade, monitoramento e resposta a incidentes.

Metodologia:

- Modelo **defense in depth** cobrindo camadas de perímetro, rede, host, aplicação, dados e identidade.
- Boas práticas de segurança em nuvem + CIS Controls como referência.
- Estrutura do plano de resposta a incidentes baseada no **NIST 800-61**.
- Premissa de **time enxuto** e **orçamento limitado** → foco em soluções simples, com quick wins.

3. Arquitetura de Defesa (Camadas)

- Diagrama – Arquitetura de Defesa em Camadas (LojaZeta)



4. Monitoramento & SIEM

Fontes de log:

- **Nginx** → acessos, erros, requisições bloqueadas pelo WAF.
- **Aplicação Node.js** → autenticações, erros de aplicação, falhas de login.
- **PostgreSQL** → queries suspeitas, falhas de autenticação.

- **Sistema Operacional** → syslog, falhas de SSH, escalonamento de privilégios.

Correlação / Casos de Uso:

1. **SQLi/XSS** → padrão de erros no DB + alertas do WAF.
2. **Brute-force** → falhas consecutivas em /login.
3. **Escalada de privilégios** → logins anômalos em servidores.
4. **Indisponibilidade** → falhas repetidas em health checks.

Alertas mínimos viáveis:

- 5 falhas de login em 1 minuto → alerta brute-force.
- Padrão de SQL injection/XSS no WAF → alerta crítico.
- Falha de backup → alerta crítico.
- Serviço (Nginx, Node.js, PostgreSQL) fora do ar → alerta crítico.

KPIs / Métricas:

- **MTTD (Mean Time to Detect):** tempo entre ataque e alerta.
- **MTTR (Mean Time to Respond):** tempo até resposta final.
- % de **cobertura de logs centralizados** (meta: 70% em 90 dias).
- Nº de **tentativas de ataque bloqueadas por WAF**.

5. Resposta a Incidentes (NIST IR)

Fluxo baseado no **NIST 800-61**:

1. **Detecção e Análise**
    a. Alertas do SIEM/WAF.
    b. Notificação por canais internos (ex.: Slack/Teams).
2. **Contenção**
    a. Bloqueio temporário de IPs maliciosos.
    b. Isolamento de instâncias comprometidas.
3. **Erradicação**
    a. Patch ou correção no código vulnerável.
    b. Remoção de backdoors/criação de novas instâncias limpas.
4. **Recuperação**
    a. Restauração a partir de backup válido.
    b. Testes de validação pós-restauração.
5. **Lições Aprendidas**

a. Registro em relatório de incidente.
b. Atualização de runbooks e regras de detecção.

Runbooks (incidentes mais prováveis):

- **SQLi/XSS:** bloquear padrão no WAF + revisão de código afetado.
- **Brute-force em /login:** bloquear IP, reforçar rate-limiting.
- **Indisponibilidade:** acionar ops, restaurar de backup/testar.

6. Recomendações (80/20) e Roadmap

Quick Wins (até 30 dias):

- Configurar WAF básico no Nginx (ou serviço gerenciado).
- Centralizar logs em um bucket/servidor de logs simples.
- Configurar alertas de brute-force, SQLi, indisponibilidade.
- Testar restauração de backup.

Médio Prazo (90 dias):

- Implementar SIEM open-source (ex.: Wazuh ou ELK stack minimalista).
- Ampliar hardening de servidores (CIS baseline).
- Criar runbooks documentados de incidentes.
- Aumentar cobertura de logs para 70%.

Longo Prazo (180 dias+):

- Automatizar respostas simples (ex.: bloqueio automático de IPs).
- Integração com autenticação multifator para identidade.
- Revisão de segurança em pipelines CI/CD.
- Simulações de incidentes (“tabletop exercises”).

Responsáveis:

- **Ops** → infraestrutura, backups, SIEM.
- **Devs** → segurança de app, correções em código.
- **Gestão** → priorização e acompanhamento de roadmap.

7. Riscos, Custos e Assunções

Riscos / Limitações:

- Time pequeno → risco de sobrecarga e atraso na resposta.
- Orçamento limitado → restrição a soluções open-source ou gerenciadas baratas.
- Logs incompletos inicialmente → pode haver lacunas na detecção.

Custos estimados:

- **Quick wins (30 dias):** praticamente zero (open-source + esforço interno).
- **90 dias:** custo de armazenamento de logs + possível VM para SIEM.
- **180 dias:** se optar por soluções SaaS (SIEM/WAF gerenciado), custo recorrente.

Suposições:

- A LojaZeta permanecerá na nuvem IaaS.
- Equipe terá tempo parcial dedicado a segurança (não full-time).
- Não há requisitos regulatórios pesados (ex.: PCI-DSS ainda não aplicável).

8. Conclusão

A LojaZeta, mesmo com equipe enxuta e orçamento restrito, pode alcançar **um salto de maturidade em segurança** com medidas de baixo custo, como WAF, centralização mínima de logs e runbooks simples de resposta.
O plano proposto oferece:

- **Defesa em profundidade** para reduzir risco de ataques mais comuns.
- **Visibilidade e monitoramento centralizado**, permitindo reação mais rápida.
- **Processo de resposta estruturado (NIST IR)**, mesmo com recursos limitados.

Próximos passos:

1. Implementar **quick wins em até 30 dias**.
2. Validar eficácia dos backups.
3. Documentar e treinar a equipe em runbooks.
4. Revisar em 6 meses os ganhos obtidos e avançar no roadmap de 180 dias.

Critério de sucesso: redução de tempo de detecção e resposta, menos falhas de login bem-sucedidas, restauração confiável de backups, e maior confiança da gestão na resiliência do ambiente.