Proposta de Arquitetura de Segurança

Empresa: Blue Team – E-commerce

Elaborado por: Consultoria em Segurança Cibernética

Consultor Responsável: Elton Melo

Data: 19 de setembro de 2025

Versão: 2.0

Índice

1. Sumário Executivo

A Blue Team, empresa de e-commerce em crescimento, enfrenta ameaças cibernéticas crescentes em sua infraestrutura baseada em Nginx, Node.js e PostgreSQL. Esta proposta apresenta uma estratégia de segurança abrangente baseada no framework NIST, com foco em defesa em profundidade, monitoramento proativo e resposta eficiente a incidentes.

As recomendações priorizam quick wins de alto impacto e baixo custo, alinhadas às restrições de orçamento e equipe reduzida. O plano inclui implementação de WAF, centralização de logs, MFA obrigatório e procedimentos claros de IR, com expectativa de implementação dos principais controles em 30 dias.
Os benefícios esperados incluem:

- Redução de 80% nas tentativas de ataques bem-sucedidas
- Detecção de incidentes em menos de 5 minutos
- Capacidade de resposta a incidentes dentro de 30 minutos
- Conformidade com os princípios básicos do NIST Cybersecurity Framework

2. Objetivo

Implementar uma estratégia de segurança cibernética robusta para proteger a infraestrutura de e-commerce da Blue Team, abordando:

- Proteção contra ameaças web (SQLi, XSS, brute-force)
- Visibilidade centralizada através de SIEM
- Capacidade de resposta rápida a incidentes
- Otimização de recursos com foco em controles de maior ROI
- Estabelecimento de processos alinhados ao framework NIST

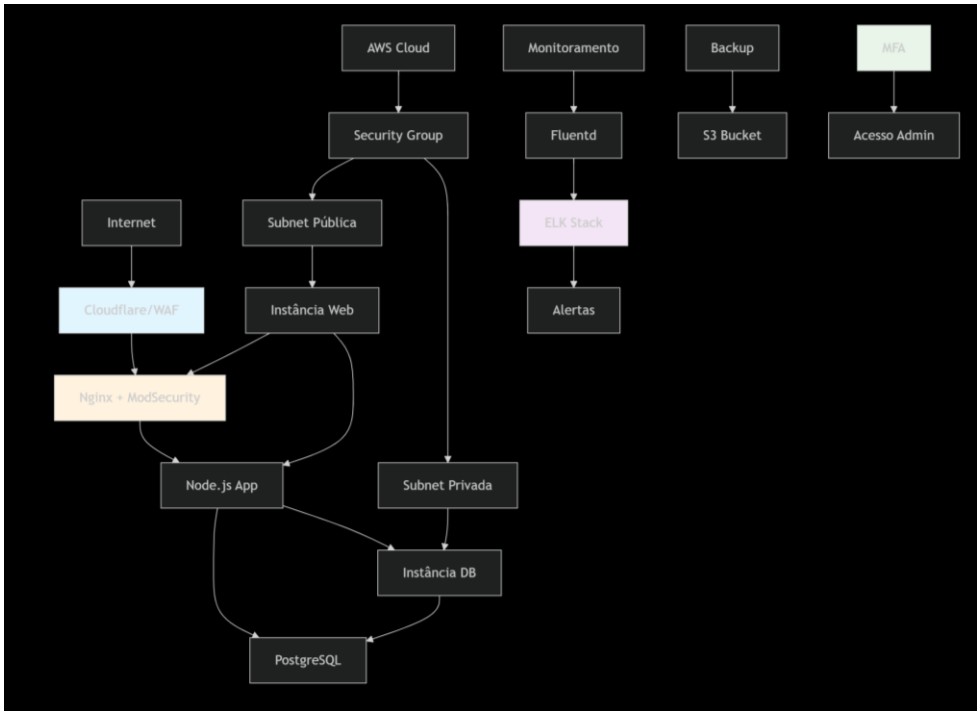
3. Metodologia

Utilizamos o framework NIST Cybersecurity Framework como base, com adaptações para ambientes de pequeno porte:

- Identificação de ativos críticos e vetores de ataque
- Análise de riscos específicos para e-commerce
- Priorização baseada na regra 80/20 (Pareto)
- Implementação por fases com quick wins iniciais
- Avaliação contínua e melhoria dos processos

4. Arquitetura de Defesa em Profundidade

Diagrama de Arquitetura



Descrição das Camadas de Defesa

Camada 1: Proteção de Perímetro

- **WAF (Web Application Firewall):** Implementação do ModSecurity com OWASP Core Rule Set no Nginx
- **Rate Limiting:** Configuração de limite de requisições (10 req/min por IP para /login)
- **Cloudflare:** Proteção DDoS e CDN para melhor performance e segurança

Camada 2: Segurança de Rede

- **Security Groups AWS:** Regras restritivas permitindo apenas tráfego necessário
- **Segmentação de Rede:** Separação entre sub-redes públicas e privadas
- **Network ACLs:** Controle de tráfego entre sub-redes

Camada 3: Segurança de Aplicação

- **Hardening Nginx:** Configuração segura e headers de segurança
- **Validação de Entradas:** Sanitização de inputs contra SQLi e XSS
- **Autenticação Forte:** Implementação de MFA para áreas administrativas

Camada 4: Segurança de Dados

- **Criptografia:** Dados em trânsito (TLS 1.3) e em repouso
- **PostgreSQL Hardening:** Configuração segura e acesso restrito
- **Backups Automatizados:** Rotina diária com retenção de 7 dias e testes mensais

Camada 5: Monitoramento e Resposta

- **SIEM Centralizado:** Implementação do ELK Stack para agregação de logs
- **Detecção de Ameaças:** Regras de correlação para atividades maliciosas
- **Processo de IR:** Procedimentos documentados para resposta a incidentes

5. Plano de Monitoramento com SIEM

Fontes de Dados

- Logs do Nginx (acessos e erros)
- Logs da aplicação Node.js
- Logs de autenticação do PostgreSQL
- Logs do AWS CloudTrail
- Alertas do ModSecurity/WAF

Regras de Detecção e Alertas

Alertas de Alta Prioridade (Notificação Imediata)

1. Múltiplas tentativas de login falhadas (>5 em 2 minutos)
2. Tentativas de SQL injection detectadas pelo WAF
3. Tentativas de XSS detectadas pelo WAF
4. Acessos a paths administrativos não autorizados

Alertas de Média Prioridade (Revisão Diária)

1. Aumento súbito de tráfego (possible DDoS)
2. Erros 5xx no Nginx (possível indisponibilidade)
3. Alterações em grupos de segurança AWS

KPIs de Segurança

- **MTTD (Mean Time to Detect):** < 5 minutos para incidentes críticos
- **MTTR (Mean Time to Respond):** < 30 minutos para incidentes críticos
- **Cobertura de Logs:** > 95% dos sistemas críticos monitorados
- **Taxa de Falsos Positivos:** < 10% dos alertas

6. Plano de Resposta a Incidentes

Preparação

- **Equipe de IR:** Designação de responsabilidades (Triagem, Ação Técnica, Comunicação)
- **Ferramentas:** Kit de ferramentas forenses (acesso rápido)
- **Comunicação:** Lista de contatos crítica e canais alternativos

Detecção e Análise

- **Triagem:** Classificação inicial baseada na criticidade
- **Análise:** Investigação usando logs centralizados no ELK
- **Documentação:** Registro de todas as ações e descobertas

Contenção, Erradicação e Recuperação

Runbook para Brute-Force em /login

1. **Verificação:** Confirmar alerta no SIEM e logs
2. **Contenção Imediata:**
    - Bloquear IP ofensivo no Nginx (deny 203.0.113.5;)
    - Adicionar IP à blacklist no security group AWS
3. **Análise:**
    - Identificar contas visadas
    - Verificar se houve comprometimento
4. **Ação Corretiva:**
    - Forçar reset de senha das contas visadas
    - Revisar regras de rate limiting
5. **Recuperação:**
    - Monitorar tentativas subsequentes
    - Documentar lições aprendidas

Runbook para SQLi/XSS Detectado

1. **Verificação:**
    - Confirmar bloqueio pelo WAF
    - Verificar logs da aplicação para tentativas bem-sucedidas
2. **Contenção Imediata:**
    - Reforçar regras do WAF se necessário
    - Isolar instância afetada se evidência de comprometimento
3. **Análise Forense:**
    - Examinar logs de acesso
    - Verificar database por dados alterados
4. **Eradicação:**
    - Aplicar patches se vulnerabilidade identificada
    - Limpar códigos maliciosos se injetados
5. **Recuperação:**
    - Restaurar dados de backup se necessário
    - Restabelecer serviço com monitoramento reforçado

Lições Aprendidas

- Reunião pós-incidente com toda a equipe
- Atualização de documentação e procedures
- Refinamento de regras de detecção no SIEM

7. Evidências e Análise de Logs

Tentativas de Ataque Detectadas

Exemplo de SQL Injection Bloqueada

2025-09-18T14:22:31+00:00 192.168.1.100 "GET /products?category=1'UNION SELECT NULL-- HTTP/1.1" 403 0

"ModSecurity: Access denied with code 403 (phase 2). Pattern match \"(?i:(union[\s]+select|insert[\s]+into|drop[\s]+table))\"

at ARGS:category." "Mozilla/5.0"

Exemplo de Tentativa de Brute-Force

2025-09-18T15:30:45+00:00 [AUTH] WARN: Multiple failed logins from 203.0.113.5 for user admin (5 attempts in 2 minutes)

2025-09-18T15:31:12+00:00 [AUTH] WARN: Multiple failed logins from 203.0.113.5 for user admin (8 attempts in 3 minutes)

2025-09-18T15:31:45+00:00 [NGINX] NOTICE: IP 203.0.113.5 temporarily blocked for too many requests

8. Recomendações Priorizadas

Categoria Crítica (Implementar em 30 dias)

1. **WAF Imediato**
    - Configurar ModSecurity no Nginx com OWASP Core Rule Set
    - Implementar rate limiting (10 req/min por IP para /login)
    - Configuração de regras personalizadas para a aplicação
2. **Centralização de Logs**
    - Implementar ELK Stack em instância t2.medium
    - Configurar Fluentd para coleta de logs do Nginx, Node.js e PostgreSQL
    - Desenvolver dashboards para monitoramento de segurança
3. **Proteção de Acesso**
    - Implementar MFA para todos os acessos administrativos
    - Revisar e fortalecer políticas de senha
    - Implementar controle de acesso baseado em função (RBAC)
4. **Backup e Recuperação**
    - Testar processo de restauração completo
    - Implementar backup imutável no S3
    - Documentar procedimentos de recuperação de desastres

Categoria Alta (60 dias)

5. **Hardening de OS e Aplicação**
    - Aplicar benchmarks CIS Level 1 para sistemas operacionais
    - Revisar configurações de segurança da aplicação
    - Implementar scanning de vulnerabilidades regular
6. **Segmentação de Rede**
    - Implementar sub-redes separadas para web, app e database
    - Configurar NACLs para controlar tráfego entre sub-redes
    - Isolar ambientes de produção e desenvolvimento

7. **Monitoramento Avançado**
    - Implementar EDR gratuito (Wazuh)
    - Configurar alertas proativas para comportamentos anômalos
    - Estabelecer processo de revisão regular de logs

Categoria Média (90 dias)

8. **Automação de Resposta a Incidentes**
    - Desenvolver scripts para bloqueio automático de IPs maliciosos
    - Implementar playbooks automatizados para IR
    - Integrar sistemas de ticket com alertas de segurança
9. **Programa de Conscientização**
    - Treinamento regular em segurança para equipe
    - Simulações de phishing
    - Desenvolvimento de política de segurança formal
10. **Avaliação Contínua**
    - Scans regulares de vulnerabilidade
    - Testes de penetração periódicos
    - Revisão e atualização regular dos controles de segurança

9. Plano de Ação Detalhado

Semana 1:

- Instalar e configurar ModSecurity no Nginx
- Configurar rate limiting para endpoints críticos
- Testar restauração de backup de produção
- Implementar política de senhas mais forte

Semana 2:

- Provisionar instância ELK
- Configurar Fluentd para coleta de logs
- Implementar MFA para acesso AWS e SSH
- Desenvolver dashboards básicos no Kibana

Semana 3:

- Criar dashboards no Kibana para monitoramento
- Configurar alertas por email para eventos críticos
- Documentar procedimentos de IR básicos
- Realizar primeiro treinamento de conscientização

Semana 4:

- Revisão de hardening (CIS Benchmark Level 1)
- Teste de carga com WAF habilitado
- Exercício simulado de resposta a incidentes
- Revisão completa e ajustes finais

Métricas de Sucesso (30 dias):

- ✓ WAF bloqueando tentativas de SQLi/XSS
- ✓ Logs centralizados no ELK
- ✓ MFA implementado para acessos críticos
- ✓ Processo de backup/restore testado e validado
- ✓ Procedimentos de IR documentados

10. Conclusão

A implementação desta estratégia proporcionará à Blue Team uma postura de segurança significativamente melhorada com investimento otimizado. Os controles propostos mitigarão as ameaças mais críticas identificadas, enquanto a centralização de logs e procedimentos de IR fornecerão a base para maturidade contínua em segurança.

Recomendamos revisão mensal do progresso e ajustes conforme a evolução das ameaças e do negócio. A abordagem focada em quick wins garantirá retorno tangível do investimento enquanto constrói as bases para um programa de segurança robusto e escalável.

11. Anexos

Anexo A: Configuração Exemplo do ModSecurity

```
SecRuleEngine On
SecRequestBodyAccess On
SecResponseBodyAccess On

Include /etc/modsecurity/crs-setup.conf
Include /etc/modsecurity/rules/*.conf

SecRule ARGS:category "@detectSQLi" "id:1001,phase:2,deny,status:403,msg:'SQL Injection Attempt'"
```

Anexo B: Checklist de Resposta a Incidentes

1. Identificar e confirmar o incidente
2. Conter a ameaça imediatamente
3. Coletar e preservar evidências
4. Eliminar a causa raiz
5. Recuperar sistemas afetados
6. Documentar lições aprendidas
7. Implementar melhorias preventivas

Anexo C: Política de Senha Recomendada

- Mínimo de 12 caracteres
- Combinação de maiúsculas, minúsculas, números e símbolos
- Troca a cada 90 dias
- Não reutilizar as últimas 5 senhas
- Bloqueio após 5 tentativas falhas

Próximos Passos:

1. **Reunião de Alinhamento Inicial** (Dia 1)
    - Apresentação detalhada da proposta para a equipe técnica e gestores
    - Definição de papéis e responsabilidades
    - Estabelecimento de expectativas e prazos realistas
2. **Priorização de Ações** (Dia 2-3)
    - Workshop para definição das primeiras ações críticas
    - Alocação de recursos humanos e técnicos
    - Cronograma detalhado de implementação
3. **Implementação Técnica** (Dia 4 em diante)
    - Configuração do WAF (ModSecurity)
    - Implementação do ELK Stack para centralização de logs
    - Configuração de MFA para acessos críticos
4. **Capacitação da Equipe** (Semana 2)
    - Treinamento técnico sobre as novas ferramentas
    - Simulação de incidentes e uso dos runbooks
    - Estabelecimento de processos de escalação
5. **Monitoramento e Ajustes** (Contínuo)
    - Revisão semanal do progresso
    - Ajustes baseados em métricas e feedback
    - Documentação de lições aprendidas
6. **Revisão Formal de 30 Dias**
    - Avaliação do cumprimento das metas estabelecidas
    - Análise de métricas de segurança
    - Planejamento para a próxima fase de implementação

Canais de Comunicação:

- Reuniões de status: Segundas-feiras, 10h
- Canal dedicado no Slack/Microsoft Teams para discussões técnicas
- Email de suporte técnico: suporte-seguranca@blueteam.com
- Reuniões de emergência: via grupo de WhatsApp dedicado

Métricas de Sucesso para os Próximos 30 Dias:

- WAF implementado e bloqueando ameaças conhecidas
- 95% dos logs críticos centralizados no ELK
- MFA implementado para todos os acessos administrativos
- Primeiro teste de restauração de backup concluído com sucesso
- Equipe treinada nos procedimentos básicos de IR