WCAP: Web Complete Application Protection

Whitepaper v0.1

Autores:

- Lucas Catão de Moraes
- Data: 03/2025

Introdução

1.1 O que é WCAP?

WCAP (Web Complete Application Protection) é um conceito inovador de segurança cibernética que propõe uma abordagem integrada e nativa para a proteção completa de aplicações web. Diferente das soluções tradicionais fragmentadas, o WCAP combina WAF (Web Application Firewall), firewall de API, proteção de e-mails, inteligência de ameaças, mitigação de DDoS e monitoramento contínuo, garantindo segurança total para aplicações web modernas.

Além disso, o WCAP incorpora o modelo de Zero Trust Security quando há autenticação de usuários. Isso significa que nenhuma requisição ou identidade é confiável por padrão, exigindo verificação contínua e autenticação reforçada antes de conceder acesso a recursos críticos. Com esse princípio, o WCAP impede acessos não autorizados e reduz a superfície de ataque ao aplicar políticas rigorosas de controle de identidade, garantindo que apenas usuários devidamente autenticados possam interagir com áreas sensíveis da aplicação.

1.2 Problema Atual

As aplicações web enfrentam diversos desafios de segurança, incluindo ataques como SQL Injection, XSS, CSRF, abuso de APIs, ataques de phishing e ataques volumétricos (DDoS). Atualmente, as empresas precisam combinar múltiplas soluções, o que gera lacunas na segurança e complexidade na implementação. Além disso, a integração entre essas soluções muitas vezes é difícil e limitada, criando um cenário onde equipes de segurança precisam configurar e monitorar diferentes sistemas que não são nativamente compatíveis entre si.

Outro grande desafio é a formação profissional necessária para que uma equipe consiga aplicar a implementação e monitoramento completo de todas essas soluções. Mesmo quando um único fabricante oferece múltiplos produtos de segurança, essas soluções geralmente não são integradas nativamente e não fazem parte de uma única solução unificada. Isso aumenta o custo operacional, demanda um alto nível de especialização técnica e pode deixar brechas de

segurança devido à falta de comunicação eficiente entre os diferentes componentes.

O WCAP resolve esse problema ao fornecer um modelo unificado e nativo de proteção, eliminando a necessidade de integrar múltiplas soluções isoladas e reduzindo a complexidade operacional e de gestão da segurança de aplicações web.

1.3 Objetivo deste Whitepaper

Este documento tem como objetivo apresentar o conceito do WCAP, sua arquitetura, princípios fundamentais e diretrizes para implementação, permitindo que empresas de tecnologia desenvolvam soluções baseadas nesse modelo. Acreditamos que esse conceito representa a evolução natural das soluções de segurança para aplicações web, substituindo o modelo tradicional baseado em WAFs complementados por diversas ferramentas isoladas. O WCAP surge como uma resposta à necessidade de um sistema de proteção integrado, eficiente e escalável, eliminando as fragilidades das abordagens atuais e fornecendo uma segurança mais completa e automatizada para o ambiente digital moderno.

2. Princípios Fundamentais do WCAP

WCAP é baseado em seis pilares principais que estabelecem diretrizes para a construção de soluções de segurança baseadas nesse conceito:

1. Proteção Nativa e Unificada → O sistema de segurança deve ser desenvolvido como um modelo integrado e nativo, eliminando a necessidade de múltiplas soluções isoladas. Toda a proteção deve ser centralizada para reduzir complexidade e melhorar eficiência.
2. Context-Aware Security → A segurança deve ser adaptativa e contextual, avaliando quem acessa, de onde, com que dispositivo e qual o comportamento esperado. Isso permite a criação de políticas dinâmicas de segurança baseadas em risco, em vez de regras estáticas.
3. Resiliência e Autoaprendizado → O modelo WCAP deve ser resiliente e capaz de se adaptar automaticamente a novas ameaças, utilizando inteligência artificial e análise comportamental para detectar e mitigar ataques antes que causem danos.
4. Zero Trust como Base de Acesso → Nenhum usuário, dispositivo ou sistema deve ser confiável por padrão. Todas as requisições devem passar por autenticação contínua e análise de segurança, garantindo que apenas entidades legítimas possam interagir com a aplicação.
5. Orquestração e Automação de Resposta → O WCAP deve permitir uma resposta automatizada e coordenada a incidentes, reduzindo tempo de reação e garantindo que ameaças sejam neutralizadas antes de se

espalharem. A integração com SIEMs e outras plataformas de monitoramento deve ser facilitada.

6. Observabilidade Total e Telemetria → Todo o tráfego, eventos e incidentes devem ser monitorados e registrados, permitindo análises avançadas e respostas mais rápidas a anomalias e padrões suspeitos. A segurança baseada em dados permite prever ataques e melhorar continuamente a eficácia da proteção.

3. Arquitetura do WCAP

3.1 Estrutura Geral

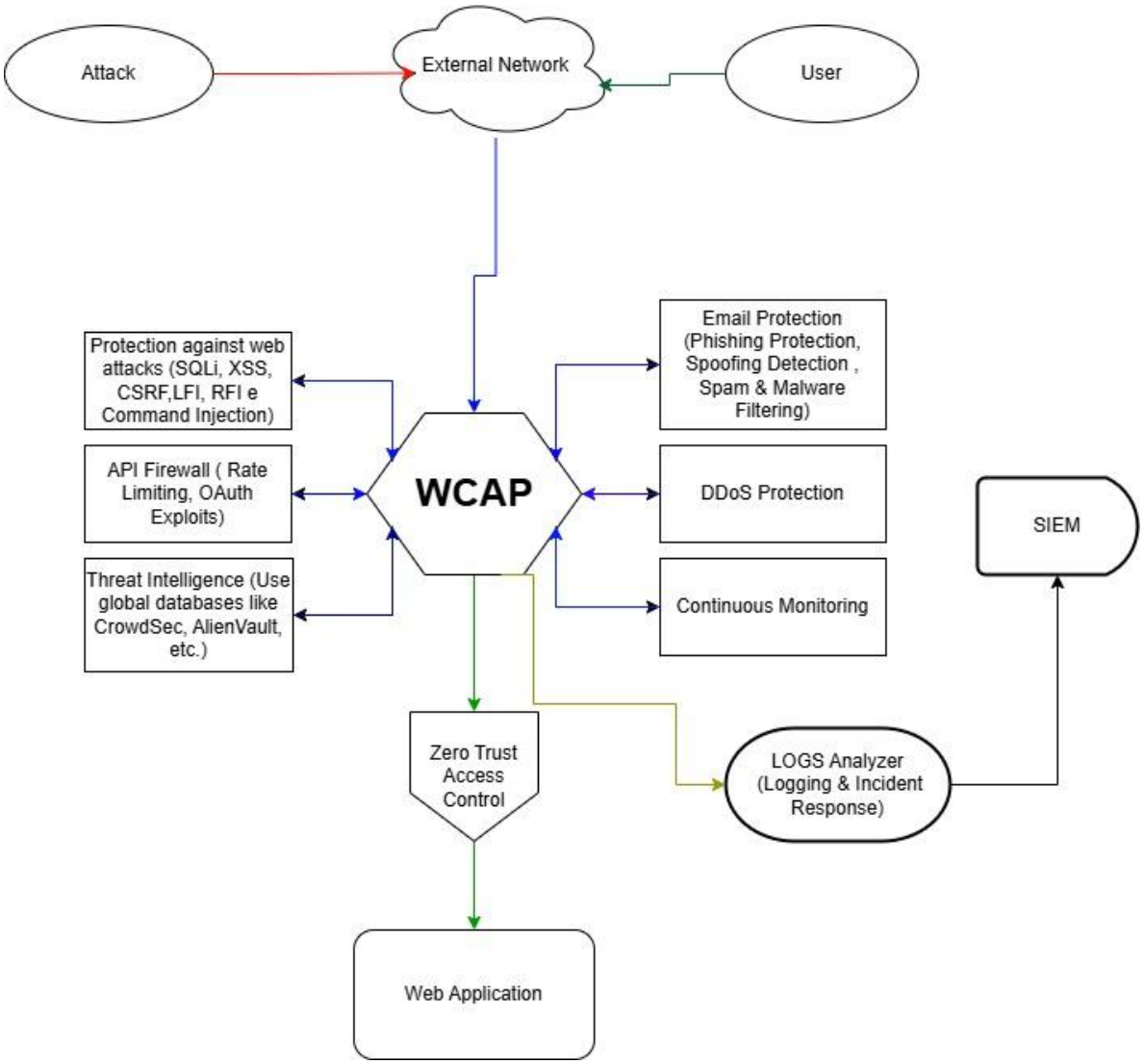
O WCAP é projetado como um modelo modular e expansível, composto por múltiplas camadas de segurança. A seguinte estrutura representa os requisitos mínimos para que uma solução possa ser considerada WCAP-compliant. No entanto, o conceito não se limita a essas camadas. Empresas podem adicionar novos componentes e funcionalidades que façam sentido dentro da proposta de segurança completa para aplicações web, desde que respeitem os princípios fundamentais do WCAP.

Estrutura Mínima WCAP-Compliant:

- **Proteção contra ataques web** (SQLi, XSS, CSRF, LFI, RFI, Command Injection).
- **Firewall de API** (Rate Limiting, OAuth Exploits).
- **Threat Intelligence** (Banco de dados globais como exemplos: CrowdSec, AlienVault, outras soluções próprias ou de terceiros).
- **Proteção de E-mails** (Phishing Protection, Spoofing Detection, Spam Filtering).
- **DDoS Protection** (Mitigação de ataques volumétricos e dirigidos).
- **Monitoramento Contínuo e Análise de Logs**.
- **Zero Trust Access Control** (Validação contínua de identidade e permissões).

Expansões opcionais: Além dessas camadas mínimas, soluções baseadas no WCAP podem incluir módulos adicionais, como prevenção contra insider threats, análise de comportamento baseada em IA, segurança em multi-cloud e respostas automáticas a incidentes, desde que sigam os princípios do WCAP de proteção nativa, contexto adaptativo e orquestração eficiente.

3.2 Diagrama da Arquitetura



4. Casos de Uso do WCAP

4.1 Aplicação em Empresas e Sites Públicos

O conceito WCAP pode ser aplicado em diversos setores que necessitam de proteção total para aplicações web, garantindo segurança, conformidade e mitigação de ameaças avançadas. Para que uma solução seja considerada WCAP-compliant, ela deve implementar todas as camadas mínimas de segurança ou mais, assegurando um ambiente seguro, resiliente e integrado. A seguir, destacamos os principais setores que se beneficiam desse modelo.

E-commerce

Os sites de e-commerce são alvos frequentes de fraudes, ataques DDoS e exploração de APIs de pagamento.

Um modelo WCAP-compliant protege lojas online garantindo:

Proteção contra fraudes e roubo de credenciais → Integração com Threat Intelligence para identificar ataques de força bruta e tentativas de login maliciosas.

Segurança para APIs de pagamento → Proteção contra abuso de APIs, exploração de OAuth e rate limiting para evitar ataques de botnets.

Defesa contra DDoS e Scraping → Bloqueio de tentativas de extrair preços, informações e dados do cliente.

Proteção de checkout e dados de pagamento → Implementação de camadas de Zero Trust e validação contínua de transações.

Bancos e Fintechs

As instituições financeiras necessitam de proteção avançada contra fraudes bancárias, roubo de identidade e ataques sofisticados.

Um WCAP-compliant fornece:

Mitigação de Phishing e Fraudes → Bloqueio de e-mails maliciosos direcionados a clientes e funcionários.

Proteção contra ataques de injeção (SQLi) e exploração de APIs → Segurança para dados bancários e interfaces críticas.

Zero Trust para Login e Autenticação → Validação contínua de sessões, comportamentos anômalos e MFA avançado.

Defesa contra DDoS direcionado → Proteção contra ataques volumétricos visando derrubar serviços bancários online.

SaaS e Aplicações Cloud

Soluções SaaS (Software as a Service) e ambientes multi-cloud exigem segurança para usuários, dados e APIs expostas.

Um WCAP-compliant fornece:

Proteção de multi-tenancy → Garantia de isolamento entre usuários e empresas dentro da plataforma SaaS.

Segurança para APIs REST/GraphQL → Rate Limiting, controle de autenticação e monitoramento de chamadas suspeitas.

Mitigação de ataques à infraestrutura Cloud → Integração com Threat Intelligence para detectar ataques direcionados.

Zero Trust para Acessos Administrativos → Garantia de que nenhuma solicitação administrativa é confiável por padrão.

Sites de Notícias e Conteúdo Aberto

Portais de notícias e conteúdo aberto devem garantir acessibilidade pública sem comprometer a segurança.

Um WCAP-compliant protege contra:

Ataques de defacement e injeção de código malicioso → Proteção contra XSS, CSRF e injeções de código.

DDoS e Scraping → Bloqueio de ataques para derrubar servidores ou copiar conteúdos protegidos.

Proteção de credenciais de administradores → Implementação de Zero Trust e MFA para gestão de conteúdos.

Segurança de APIs de publicação e distribuição → Controle sobre APIs que enviam, publicam e compartilham notícias.

Governo e Infraestrutura Crítica

Entidades governamentais e infraestruturas críticas (energia, telecomunicações, saúde) enfrentam riscos elevados de ataques cibernéticos, espionagem e sabotagem digital.

Soluções WCAP-compliant garantem:

Zero Trust para portais governamentais e infraestrutura crítica → Nenhuma requisição é confiável por padrão, garantindo autenticação contínua e controle rígido de acesso.

Proteção de APIs e serviços públicos → Prevenção contra ataques de injeção, exploração de endpoints críticos e manipulação de dados.

Monitoramento contínuo e inteligência de ameaças → Integração com Threat Intelligence para prever e bloquear ataques direcionados.

Resiliência contra ataques patrocinados por estados e APTs (Advanced Persistent Threats) → Análise de padrões maliciosos e resposta automatizada a ameaças persistentes.

Defesa contra ataques DDoS direcionados a sistemas governamentais → Mitigação de tentativas de derrubar serviços críticos, como sistemas de votação eletrônica, bases de dados nacionais e redes de telecomunicações.

Saúde e Hospitais

O setor de saúde depende de disponibilidade e integridade de dados para operações críticas, tornando-se um alvo, roubo de dados e manipulação de registros médicos.

Soluções WCAP-compliant garantem:

Zero Trust para acesso a registros médicos eletrônicos (EMR) → Nenhum acesso deve ser confiável sem autenticação forte e análise de comportamento.

Segurança para APIs de telemedicina e dispositivos médicos conectados (IoT) → Monitoramento contínuo para prevenir acessos não autorizados e ataques a dispositivos clínicos.

DDoS Protection para garantir continuidade operacional → Prevenção contra ataques que interrompam o funcionamento de hospitais e clínicas.

Inteligência de ameaças aplicada a dados de saúde → Análise contínua de padrões suspeitos em requisições a bancos de dados médicos.

Educação e Universidades

Instituições acadêmicas operam ambientes dinâmicos e descentralizados, tornando-se alvos de roubo de credenciais, ataques de phishing e exploração de redes educacionais.

Soluções WCAP-compliant garantem:

Zero Trust para alunos, professores e pesquisadores → Implementação de autenticação contínua e segmentação de acesso.

Proteção contra vazamento de dados acadêmicos → Controle rigoroso de acessos a repositórios de pesquisas e dados sensíveis.

Segurança para plataformas EAD (Educação a Distância) → Prevenção contra ataques de injeção e exploração de APIs de cursos online.

DDoS Protection para garantir disponibilidade de plataformas educacionais → Monitoramento e mitigação de tentativas de interrupção de serviços acadêmicos.

Setor de Jogos e Streaming

Plataformas de jogos online e serviços de streaming são alvos de ataques DDoS, exploração de APIs e roubos de credenciais de jogadores e assinantes.

Soluções WCAP-compliant oferecem:

Proteção contra ataques volumétricos (DDoS) em tempo real → Monitoramento e mitigação automática de tentativas de interrupção de servidores de jogos e streaming.

Zero Trust para login e autenticação → Implementação de controle contínuo de acessos suspeitos e prevenção contra fraudes em contas.

Proteção de APIs para matchmaking e transações → Segurança contra manipulação de jogos online e exploração de APIs de pagamentos.

Monitoramento contínuo de tráfego malicioso → Inteligência de ameaças para detectar e bloquear comportamentos abusivos e ataques automatizados.

4.2 Zero Trust aplicado ao WCAP

O conceito de Zero Trust dentro do WCAP-compliant garante que nenhuma requisição, usuário ou dispositivo seja confiável por padrão, exigindo autenticação contínua, análise de comportamento e monitoramento de segurança adaptativo. O Zero Trust aplicado ao WCAP estrutura um modelo de segurança contínuo e adaptativo, onde o acesso a aplicações web, APIs, dados sensíveis e painéis administrativos é constantemente validado.

Como o WCAP implementa Zero Trust

Tráfego Público vs. Tráfego Autenticado

Para garantir um controle eficiente de acessos, o WCAP diferencia tráfego público e tráfego autenticado, aplicando políticas específicas:

Tráfego Público: Qualquer solicitação não autenticada segue um fluxo de validação de reputação, que pode incluir Threat Intelligence, detecção de tráfego anômalo, análise de IPs suspeitos e heurísticas de navegação.

Tráfego Autenticado: Qualquer requisição autenticada passa por múltiplas camadas de verificação, incluindo autenticação contínua, análise de comportamento do usuário, reputação do dispositivo e conformidade com políticas de segurança.

Diferença entre tráfego público e autenticado dentro do WCAP:

Requisição	Validação pelo WCAP
Visitante anônimo acessando site público	Reputação do IP, detecção de bots, análise de comportamento
Usuário autenticado acessando área restrita	MFA, análise contínua de sessão, validação de dispositivo
Chamada para APIs críticas	Autenticação via OAuth, validação de integridade, rate limiting
Administrador acessando painel de controle	MFA, Zero Trust Access Control, análise de localização e comportamento

Aplicação de Políticas de Autenticação Contínua

O WCAP exige autenticação contínua, o que significa que um usuário ou sistema não mantém acesso indefinido sem validação. Isso pode ser implementado da seguinte forma:

Revalidação periódica da sessão → Tokens de acesso expiram em ciclos curtos e exigem reautenticação baseada em risco.

MFA dinâmico → Quando um usuário acessa de um novo local, dispositivo ou comportamento suspeito, o sistema exige autenticação reforçada.

Monitoramento de sessão → Se um usuário autenticado apresentar comportamento anômalo (ex: acessos a múltiplas contas rapidamente), o WCAP pode forçar um novo login ou bloquear o acesso

Implementação de Zero Trust no WCAP-Compliant

Para uma implementação eficaz de Zero Trust dentro do WCAP, é necessário estruturar os seguintes elementos:

Política de Identidade e Acesso (IAM) → Criar regras rigorosas para acesso de usuários e dispositivos.

Autenticação Adaptativa → Aplicar autenticação baseada em contexto, risco e comportamento do usuário.

Microsegmentação → Criar regras que garantam que mesmo usuários autenticados só tenham acesso ao necessário.

Monitoramento Contínuo e Análise de Comportamento → Validar a sessão do usuário em tempo real e aplicar políticas dinâmicas.

Proteção para APIs e Webhooks → Aplicar regras específicas para prevenir acessos indevidos a endpoints críticos.

Threat Intelligence Integrado → Rejeitar acessos que possuam padrões conhecidos de ataques, IPs maliciosos e tentativas de exploração de APIs.

Quando aplicar Zero Trust dentro do WCAP?

Zero Trust deve ser aplicado sempre que houver autenticação ou interação com dados sensíveis. Casos de uso dentro do WCAP:

Painéis Administrativos → Proteção contra sequestro de sessões e ataques de força bruta.

APIs Públicas e Privadas → Evita exposição de dados e exploração por terceiros maliciosos.

Usuários de Alto Risco → Aplicação de regras adicionais para usuários que acessam de locais ou dispositivos suspeitos.

Sessões Longas e Persistentes → Forçar renovação periódica e validação contínua de credenciais.

Estruturando Zero Trust no WCAP

Para que uma solução WCAP-compliant implemente corretamente Zero Trust, é necessário um modelo de camadas de segurança:

Camada 1: Identidade e Acesso

MFA obrigatório para acessos administrativos e críticos.

Validação de dispositivos confiáveis e histórico de acessos.

Camada 2: Monitoramento Contínuo e Análise de Sessão

Uso de Machine Learning e AI para detectar acessos suspeitos.

Monitoramento em tempo real de tráfego autenticado e não autenticado.

Camada 3: Restrições Granulares e Resposta a Incidentes

Aplicação de políticas de acesso baseadas no princípio do menor privilégio.

Detecção automática de tentativas de movimentação lateral e ataques internos.

Respostas automáticas como encerramento de sessão, bloqueio de IP e notificações.

A implementação de Zero Trust no WCAP garante que todas as interações com aplicações web e APIs sejam constantemente validadas, reduzindo fraudes, acessos indevidos e vulnerabilidades. Empresas que adotam o WCAP-compliant com Zero Trust garantem proteção nativa e adaptativa, eliminando riscos associados a credenciais comprometidas, movimentação lateral e sequestro de sessões.

5. Comparação com Soluções Tradicionais

5.1 Diferença entre WCAP e WAF Tradicional

As soluções de segurança tradicionais, como WAFs isolados, SIEMs e firewalls de API, tentam mitigar riscos cibernéticos, mas falham ao fornecer uma abordagem unificada e adaptável para a proteção de aplicações web. O WCAP-compliant resolve esses problemas integrando proteção nativa e camadas avançadas de segurança, eliminando as fragilidades das soluções segmentadas.

Por que migrar para soluções WCAP-compliant?

A arquitetura WCAP oferece segurança contínua, integrada e automatizada, enquanto soluções tradicionais frequentemente dependem de múltiplos produtos desconectados, resultando em lacunas de proteção e desafios operacionais.

Característica	WCAP	WAF Tradicional
Proteção de API	Sim – Protege APIs de maneira nativa, implementando **rate limiting, autenticação e segurança de endpoints**.	Não – Apenas protege tráfego HTTP, sem considerar APIs REST ou GraphQL.
Proteção de E-mails	Sim – Integrado com inteligência de ameaças para detectar **phishing, spoofing e malwares em e-mails**.	Não – WAFs não oferecem proteção contra ameaças veiculadas por e-mail.
Inteligência de Ameaças	Sim – Usa **AI e feeds globais** para antecipar ameaças antes de impactar a aplicação.	Limitado – Apenas bloqueia padrões de ataques conhecidos, sem análise preditiva.
Zero Trust	Sim – Implementa **autenticação contínua e restrição de acessos não confiáveis**.	Não – WAFs não realizam controle contínuo de identidade.
Orquestração de Resposta	Sim – Automatiza **bloqueios, resposta a incidentes e contenção de ataques**.	Não – Apenas alerta, sem automação de mitigação.
DDoS Protection Avançado	Sim – Mitiga ataques volumétricos e de camada 7 com **inteligência adaptativa**.	Limitado – Apenas bloqueia padrões básicos de DDoS.
Análise Comportamental e Resposta Automática	Sim – Monitora **comportamento de usuários e tráfego** para identificar **ameaças avançadas**.	Não – WAFs analisam apenas requisições individuais, sem contexto.
Monitoramento Contínuo e Telemetria	Sim – Inclui **registro detalhado de eventos, tráfego e tentativas de ataque em tempo real**.	Limitado – Pode gerar logs, mas sem análise profunda e contínua.
Proteção contra Exploração de APIs OAuth e Tokens JWT	Sim – Valida continuamente **uso indevido de credenciais e manipulação de tokens**.	Não – WAFs não possuem inteligência para detectar exploração avançada de autenticação.

Argumentação para Construção de Soluções com WCAP

Redução de Complexidade Operacional

Soluções tradicionais exigem múltiplos produtos para cobrir diferentes vetores de ataque (exemplo: WAF + firewall de API + ferramentas de proteção de e-mails). Isso gera integrações complexas, custos elevados e pontos cegos na segurança. O WCAP-compliant elimina essa fragmentação, fornecendo um modelo unificado de proteção.

Segurança Adaptativa e Inteligente

Enquanto um WAF tradicional depende de regras fixas e assinaturas de ameaças conhecidas, o WCAP aplica inteligência preditiva, usando Machine Learning e análise de comportamento para antecipar ataques. Isso significa menor dependência de regras estáticas e mais capacidade de detectar ataques inéditos.

Implementação Nativa de Zero Trust

A maioria dos WAFs tradicionais não aplica Zero Trust, deixando vulnerabilidades em acessos internos e tráfego autenticado. O WCAP-compliant implementa autenticação contínua, restrições de acesso dinâmicas e segmentação rigorosa, garantindo que nenhuma identidade ou dispositivo seja confiável por padrão.

Automação de Resposta e Remediação

WAFs podem gerar alertas, mas não bloqueiam ameaças de forma proativa. O WCAP é projetado para reagir automaticamente a incidentes, bloqueando tráfego malicioso e isolando ameaças em tempo real.

Maior Eficiência na Proteção de APIs

O tráfego de APIs é fundamental para aplicações modernas, mas WAFs tradicionais não possuem inteligência para proteger chamadas de API contra abusos e ataques direcionados. O WCAP-compliant inclui firewall de API nativamente, protegendo autenticação OAuth, tokens JWT e prevenindo abuso de endpoints.

A adoção de soluções WCAP-compliant permite que empresas reduzam sua complexidade operacional, melhorem a resposta a incidentes e eliminem vulnerabilidades deixadas por soluções tradicionais. Diferente do modelo fragmentado de WAF + firewalls adicionais, o WCAP integra proteção completa, automação e inteligência adaptativa, tornando-se o novo padrão de segurança para aplicações web.

Implementação do WCAP

Objetivo: Fornecer diretrizes técnicas para empresas desenvolverem soluções baseadas no WCAP, garantindo conformidade com os princípios fundamentais do conceito. Esta seção estabelece requisitos mínimos, frameworks recomendados e melhores práticas para a criação de sistemas WCAP-compliant, permitindo que desenvolvedores, arquitetos de segurança e fornecedores de tecnologia implementem o modelo de maneira eficaz.

Diretrizes para Desenvolvimento

Para que uma solução seja WCAP-compliant, ela deve atender a um conjunto de requisitos mínimos e oferecer opções de expansão, garantindo segurança contínua e escalabilidade. A seguir, definimos as diretrizes essenciais para desenvolvimento.

Uma solução WCAP deve conter **todas as camadas fundamentais** para ser considerada WCAP-compliant.

Estes são os requisitos essenciais:

Proteção de Aplicações Web → Implementação de firewall de aplicação (WAF) para mitigar ataques como SQL Injection, XSS, CSRF, LFI/RFI, e exploração de falhas em headers HTTP.

Proteção de APIs → Firewall de API nativo, com rate limiting, autenticação via OAuth, monitoramento de tráfego API e proteção contra ataques a endpoints.

Inteligência de Ameaças Integrada → Capacidade de utilizar feeds globais (ex: CrowdSec, AlienVault), machine learning e análise preditiva para antecipação de ataques.

DDoS Protection Avançado → Implementação de camadas de mitigação contra ataques volumétricos (L3/L4) e ataques de aplicação (L7).

Zero Trust Access Control → Aplicação de controle de acesso contínuo, autenticação adaptativa e segmentação de permissões.

Monitoramento e Resposta a Incidentes → Registro detalhado de logs, correlação de eventos, automação de resposta e integração com SIEMs.

Proteção contra Phishing e E-mails Maliciosos → Monitoramento de tráfego de e-mails para identificação de ataques como spoofing, phishing e BEC (Business Email Compromise).

Orquestração e Automação de Segurança → Adoção de playbooks de resposta automatizada, políticas de mitigação em tempo real e análise comportamental.

Estruturação do Desenvolvimento

Proteção de Aplicações Web

OWASP:

- Aplicar os controles definidos no OWASP Top 10 para mitigar vulnerabilidades como SQL Injection (A03:2021), XSS (A07:2021), CSRF e quebras de autenticação (A07:2021).
- Implementar cabeçalhos de segurança conforme OWASP Security Headers Project, incluindo Content Security Policy (CSP), Strict-Transport-Security (HSTS) e X-Frame-Options.
- Para APIs, seguir o OWASP API Security Top 10, protegendo endpoints contra autenticação fraca, vazamento de dados e falhas de autorização.

MITRE ATT&CK:

- Mapear táticas e técnicas da matriz MITRE ATT&CK, como T1190 (Exploração de Aplicações Web), T1071.001 (C2 via HTTP) e T1133 (Acesso Remoto Externo).
- Integrar automação para resposta ativa a ataques baseados nos padrões de técnicas MITRE ATT&CK.

CIS Controls:

- Aplicação obrigatória dos CIS Control 3 (Proteção de Aplicações Web e Serviços de Email) e CIS Control 11 (Defesa Contra Ataques na Web).
- Implementação de monitoramento contínuo conforme CIS Control 6 (Monitoramento de Logs e Eventos).

Zero Trust (NIST SP 800-207):

- Garantir que todas as requisições passem por autenticação rigorosa e validação contínua de identidade, eliminando confiança implícita.
- Utilizar segmentação para evitar movimentação lateral e limitar acessos de aplicações a somente o necessário.

Proteção de APIs

OWASP:

- Seguir as recomendações do OWASP API Security Top 10, incluindo proteção contra API Injection (API3:2023) e Excessive Data Exposure (API2:2023).
- Aplicar OAuth 2.0 e OpenID Connect para autenticação robusta de clientes e usuários.

MITRE ATT&CK:

- Monitoramento de padrões maliciosos baseados em T1190 (Exploração de Aplicações Web) e T1071.001 (C2 via HTTP).
- Aplicação de análise de tráfego API para detecção de comportamento anômalo em chamadas repetitivas ou tentativas de enumeração de endpoints.

Zero Trust:

- Nenhuma API deve ser acessível sem autenticação contínua.
- Aplicação de Rate Limiting dinâmico e restrição de permissões baseadas em funções e políticas de segurança.

Inteligência de Ameaças Integrada

MITRE ATT&CK:

- T1087.002 (Enumeração de Contas de Usuário - Nuvem) → Identificar tentativas de reconhecimento contra aplicações e APIs.
- T1190 (Exploração de Aplicações Web) → Mapeamento de padrões de exploração com base em inteligência de ameaças.
- T1071.001 (C2 via HTTP) → Monitoramento de tráfego suspeito que simula comunicações de comando e controle.
- T1203 (Exploração de Software Cliente) → Identificação de ataques explorando vulnerabilidades conhecidas.

CIS Controls:

- CIS Control 6 (Monitoramento e Análise de Eventos) → Implementação obrigatória de SIEMs e correlação de eventos de segurança para identificação de ataques emergentes.
- CIS Control 7 (Proteção contra Malware) → Integração com feeds de inteligência de ameaças para bloqueio preventivo de arquivos suspeitos e domínios maliciosos.

Zero Trust:

- Threat Intelligence Feeds → Integração contínua com bases globais de IPs maliciosos, listas de domínios bloqueados e assinaturas de ataques para bloqueios em tempo real.
- Adaptive Trust Policies → Implementação de políticas dinâmicas que ajustam permissões e bloqueios com base em inteligência contextual e análise de risco.

DDoS Protection Avançado

OWASP:

- OWASP API Security Top 10 (API4:2023 - Lack of Rate Limiting) → Aplicação de rate limiting para evitar abuso de requisições maliciosas.
- OWASP Application Security Verification Standard (ASVS) → Implementação de controles para validação de tráfego legítimo e mitigações contra injeções de pacotes massivos.

MITRE ATT&CK:

- T1498 (Ataque de Negação de Serviço - DoS) → Monitoramento e mitigação de ataques que exploram recursos computacionais para degradar o desempenho de sistemas.
- T1499 (Ataque de Negação de Serviço Distribuído - DDoS) → Detecção e resposta a ataques volumétricos e de exaustão de serviços.
- T1498.001 (Negação de Serviço Baseada em Rede) → Proteção contra ataques de amplificação e exploração de protocolos inseguros.
- T1498.002 (Negação de Serviço Baseada em Aplicação) → Identificação de ataques HTTP Flood e ataques direcionados à camada 7.

CIS Controls:

- CIS Control 12 (Defesa Contra Ataques na Rede) → Aplicação de filtragem e inspeção profunda de pacotes (DPI) para mitigar ataques de camada 3 a 7.
- CIS Control 13 (Segurança de Fronteira) → Implementação de soluções de mitigação automatizadas contra anomalias de tráfego, bloqueando ataques em tempo real.

Zero Trust:

- Reputação de IP e Monitoramento Contínuo → Nenhuma requisição deve ser processada sem avaliação de reputação do IP, ASN e correlação com inteligência de ameaças.
- Autenticação Adaptativa → Implementação de autenticação forte para tráfego suspeito, exigindo MFA ou captchas avançados em requisições anômalas.

Zero Trust Access Control

Zero Trust (NIST SP 800-207):

- Continuous Authentication & Least Privilege Access → Cada requisição deve ser autenticada dinamicamente com base em análise de comportamento, identidade e risco associado.

- Microsegmentação e Políticas Granulares → Nenhum usuário ou serviço deve ter acesso sem autorização explícita para aquele recurso específico.

MITRE ATT&CK:

- T1078 (Uso de Credenciais Válidas) → Monitoramento contínuo de logins suspeitos, incluindo acessos de locais ou dispositivos não reconhecidos.
- T1566.001 (Phishing com Links Maliciosos) → Aplicação de políticas contra tentativas de roubo de credenciais e detecção de tentativas de login com credenciais vazadas.
- T1021.001 (Uso de RDP para Movimentação Lateral) → Bloqueio de acessos não autorizados a serviços administrativos e controle de sessão de usuários privilegiados.

CIS Controls:

- CIS Control 16 (Segurança de Conta e Gestão de Senhas) → Aplicação de políticas de autenticação forte (MFA, senhas seguras e tokens adaptativos).
- CIS Control 5 (Proteção de Contas Privilegiadas) → Restrição rigorosa para contas administrativas e monitoramento contínuo de sessões elevadas.

Monitoramento e Resposta a Incidentes

OWASP:

- OWASP Application Security Verification Standard (ASVS) → Aplicação de requisitos de verificação para coleta e análise de logs de segurança, detecção de anomalias e resposta a eventos suspeitos.
- OWASP Top 10 (A09:2021 – Falhas de Registro e Monitoramento de Segurança) → Garantia de que todos os eventos críticos são devidamente registrados e analisados para resposta rápida.

MITRE ATT&CK:

- T1057 (Descoberta de Processos em Execução) → Monitoramento de processos para identificar comportamento suspeito em servidores web e aplicações.
- T1071.001 (C2 via HTTP/S) → Identificação de tráfego de comando e controle (C2) mascarado em conexões HTTPS legítimas.
- T1020 (Exfiltração de Dados pela Rede) → Monitoramento de tentativas de vazamento de informações sensíveis.

- T1562.004 (Evasão de Logs de Segurança) → Identificação e bloqueio de tentativas de adulteração ou remoção de logs críticos.

CIS Controls:

- CIS Control 6 (Monitoramento e Análise de Eventos) → Implementação obrigatória de SIEMs e correlação de eventos de segurança.
- CIS Control 19 (Resposta a Incidentes e Gestão de Recuperação) → Procedimentos estruturados para resposta rápida a incidentes de segurança.
- CIS Control 8 (Gestão de Auditoria e Logs) → Armazenamento seguro e análise contínua de logs críticos para rastreamento forense.

Zero Trust:

- Monitoramento Contínuo de Sessões → Detecção de acessos anômalos e comportamento suspeito.
- Resposta Automatizada → Adoção de ações imediatas, como isolamento de sessões, encerramento de conexões suspeitas e alerta de incidentes.
- Integração com SOAR → Orquestração de respostas automatizadas e mitigação de ameaças.

Proteção contra Phishing e E-mails Maliciosos

OWASP:

- OWASP Phishing Defense Cheat Sheet → Implementação de políticas de proteção contra phishing, incluindo filtros de reputação e análise de padrões de e-mails suspeitos.
- OWASP Top 10 (A04:2021 - Design Inseguro) → Aplicação de controles para prevenir a manipulação de fluxos de e-mail e injeção de dados maliciosos.

MITRE ATT&CK:

- T1566.001 (Phishing com Links Maliciosos) → Identificação de e-mails que contêm URLs maliciosas ou engenharia social.
- T1566.002 (Phishing com Anexos Maliciosos) → Detecção e análise de arquivos anexados que exploram vulnerabilidades de software.
- T1583.003 (Registro de Domínios para Engenharia Social) → Monitoramento de domínios recém-registrados usados para ataques de phishing.

- T1204.001 (Execução de Código via E-mail) → Identificação de arquivos ou macros maliciosas que exploram vulnerabilidades no cliente de e-mail.

CIS Controls:

- CIS Control 3 (Proteção Contra Engenharia Social e Phishing) → Implementação de filtros avançados de conteúdo para detecção de ataques de phishing.
- CIS Control 9 (Proteção de Serviços de Email) → Aplicação obrigatória de SPF, DKIM e DMARC para validação de remetentes e prevenção de spoofing.
- CIS Control 13 (Segmentação de Segurança) → Isolamento de e-mails maliciosos para quarentena e análise.

Orquestração e Automação de Segurança

OWASP:

- OWASP Automated Threats to Web Applications (OAT) → Implementação de mecanismos de deteção e resposta automatizada contra ameaças web.
- OWASP Application Security Verification Standard (ASVS) → Aplicação de controles para autenticação contínua, automação de mitigação e resposta adaptativa a incidentes.

MITRE ATT&CK:

- T1078 (Uso de Credenciais Válidas) → Identificação de credenciais comprometidas em tempo real e resposta automatizada.
- T1562.001 (Desativação de Controles de Segurança) → Monitoramento de tentativas de desativação de firewalls, WAFs e agentes de segurança.
- T1489 (Encerramento de Serviço) → Bloqueio de tentativas de desligamento de servidores críticos por atacantes.

CIS Controls:

- CIS Control 18 (Automação de Respostas e Playbooks de Segurança) → Implementação de SOARs para resposta a incidentes de forma automatizada.
- CIS Control 14 (Gerenciamento de Permissões e Acessos) → Aplicação de controles para ajustar automaticamente privilégios de usuários conforme comportamento e risco.

- CIS Control 16 (Segurança de Conta e Gestão de Senhas) → Automatização da revogação de credenciais vazadas, bloqueio de contas suspeitas e reforço de MFA baseado em riscos.

Zero Trust:

- Resposta Automatizada Baseada em Comportamento → Ações como bloqueio dinâmico de IPs, revogação de sessões e exigência de reautenticação.
- Integração com IA para Detecção de Anomalias → Uso de Machine Learning para prever ameaças antes de sua execução.
- Redução de Falsos Positivos → Ajuste adaptativo de regras com base no histórico de ameaças reais.

Cada camada de proteção do WCAP deve ser construída com base nas melhores práticas definidas por frameworks reconhecidos internacionalmente, garantindo segurança robusta e adaptável.

A construção de soluções WCAP-compliant exige uma abordagem modular, integrada e alinhada com as melhores práticas do setor de cibersegurança. Empresas que adotam esse modelo garantem proteção avançada, automação de segurança e resiliência contra-ataques modernos.

Integração com SIEM e Logs

Fluxo de Processamento de Logs:

Os logs devem ser gerados por múltiplas camadas do WCAP, incluindo:

- **Firewall de Aplicação (WAF/WCAP)** → Captura tentativas de SQL Injection, XSS, CSRF, LFI/RFI e ataques à autenticação.
- **Proteção de APIs** → Registra acessos a endpoints críticos, tentativas de Rate Limit Bypass, abusos de OAuth e explorações de JWT.
- **Monitoramento de Sessões e Autenticação** → Registra tentativas de login suspeitas, MFA inválido e credenciais comprometidas.
- **Proteção contra DDoS** → Gera métricas de requisições anômalas, tráfego volumétrico, TCP SYN Floods, HTTP Flood e anomalias no tempo de resposta.
- **E-mails e Phishing** → Captura tentativas de phishing, spoofing, anexos suspeitos e ataques de engenharia social.

- **Orquestração e Automação** → Logs de ações automatizadas realizadas pelo SOAR (bloqueios, respostas a incidentes, contenção de ameaças).

Transmissão para SIEM

Os logs coletados devem ser transmitidos de forma segura para um SIEM centralizado. Os métodos mais comuns incluem:

Syslog (UDP/TCP 514) → Usado para envio direto para SIEMs como Splunk, QRadar, Wazuh.

APIs de Log (Webhook, RESTful API) → Transmissão em tempo real para plataformas SIEM em cloud como Elastic Security e AWS GuardDuty.

Agentes de Log (Filebeat, Fluentd, Wazuh Agent) → Captura de logs locais e envio para análise centralizada.

Kafka / Message Queues → Para ambientes de alto volume, logs são enviados para um broker de mensagens, permitindo processamento escalável.

Processamento e Enriquecimento

Nesta fase, os logs devem ser normalizados, analisados e correlacionados com inteligência de ameaças:

Parsing e Normalização → Conversão de logs brutos para um formato estruturado (JSON, ECS - Elastic Common Schema).

Enriquecimento com Threat Intelligence Feeds:

- OpenCTI, AlienVault OTX, CrowdSec: Verificação de IPs, domínios e hashes maliciosos.
- Análise de reputação de IPs e ASN: Bloqueio dinâmico de tráfego suspeito.
- Cross-check de credenciais vazadas: Identificação de usuários comprometidos com bases como Have I Been Pwned.

Identificação de Comportamentos Anômalos: Machine Learning aplicado para detectar padrões suspeitos:

- Usuário acessando de diferentes países em curtos intervalos (impossível geograficamente).
- Aumento repentino de requisições HTTP incomuns.
- Tentativas de autenticação sucessivas sem MFA.

POCs Adicionados em Anexo GitHub