WCAP: Web Complete Application Protection

Whitepaper v0.1

Authors:
- Lucas Catão de Moraes
- Date: 03/2025

Introduction

1.1 What is WCAP?

WCAP (Web Complete Application Protection) is an innovative cybersecurity concept that proposes a fully integrated and native approach to comprehensive web application protection. Unlike traditional fragmented solutions, WCAP combines a Web Application Firewall (WAF), API firewall, email protection, threat intelligence, DDoS mitigation, and continuous monitoring—ensuring complete security for modern web applications.

Moreover, WCAP incorporates the Zero Trust Security model whenever user authentication is involved. This means that no request or identity is trusted by default, requiring continuous verification and strong authentication before granting access to critical resources. With this principle, WCAP prevents unauthorized access and reduces the attack surface by enforcing strict identity control policies, ensuring that only properly authenticated users can interact with sensitive areas of the application.

1.2 Current Problem

Web applications face a wide range of security challenges, including attacks such as SQL Injection, XSS, CSRF, API abuse, phishing, and volumetric attacks (DDoS). Currently, organizations must rely on a combination of multiple solutions, which creates security gaps and increases implementation complexity. Moreover, integrating these solutions is often difficult and limited, leading to a scenario in which security teams must configure and monitor different systems that are not natively compatible with each other.

Another major challenge lies in the level of professional training required for a team to successfully implement and monitor all these solutions. Even when a single vendor offers multiple security products, they are often not natively integrated or part of a unified solution. This increases operational costs, demands a high level of technical expertise, and can leave security vulnerabilities due to the lack of efficient communication between components.

WCAP addresses this issue by providing a unified and native protection model, eliminating the need to integrate multiple isolated solutions and reducing the operational and management complexity of web application security.

1.3 Purpose of this Whitepaper

This document aims to present the WCAP concept, its architecture, core principles, and implementation guidelines, enabling technology companies to develop solutions based on this model. We believe this concept represents the natural evolution of web application security solutions, replacing the traditional model centered around WAFs supplemented by various isolated tools.

WCAP emerges as a response to the need for an integrated, efficient, and scalable protection system—eliminating the weaknesses of current approaches and delivering more comprehensive and automated security for the modern digital environment.

2. Core Principles of WCAP

WCAP is based on six core pillars that serve as guidelines for the development of security solutions grounded in this concept:

1. **Native and Unified Protection** → The security system must be designed as an integrated and native model, eliminating the need for multiple isolated solutions. All protection should be centralized to reduce complexity and improve efficiency.
2. **Context-Aware Security** → Security must be adaptive and contextual, evaluating who is accessing, from where, with which device, and what the expected behavior is. This enables the creation of dynamic risk-based security policies instead of relying on static rules.
3. **Resilience and Self-Learning** → The WCAP model must be resilient and capable of automatically adapting to new threats by leveraging artificial intelligence and behavioral analysis to detect and mitigate attacks before damage occurs.
4. **Zero Trust as the Foundation for Access** → No user, device, or system should be trusted by default. All requests must go through continuous authentication and security analysis, ensuring that only legitimate entities can interact with the application.
5. **Orchestration and Automated Response** → WCAP should enable an automated and coordinated response to incidents, reducing reaction time and ensuring threats are neutralized before they spread. Integration with SIEMs and other monitoring platforms should be seamless.
6. **Full Observability and Telemetry** → All traffic, events, and incidents must be monitored and logged, enabling advanced analytics and quicker responses to anomalies and suspicious patterns. Data-driven security makes it possible to predict attacks and continuously improve protection effectiveness.

3. WCAP Architecture

3.1 General Structure

WCAP is designed as a modular and expandable model, composed of multiple layers of security. The following structure represents the **minimum requirements** for a solution to be considered WCAP-compliant. However, the concept is not limited to these layers—organizations may add new components and features that align with the goal of comprehensive web application security, as long as they adhere to WCAP's core principles.

Minimum WCAP-Compliant Structure:

- **Web Attack Protection** (SQLi, XSS, CSRF, LFI, RFI, Command Injection)
- **API Firewall** (Rate Limiting, OAuth Exploits)

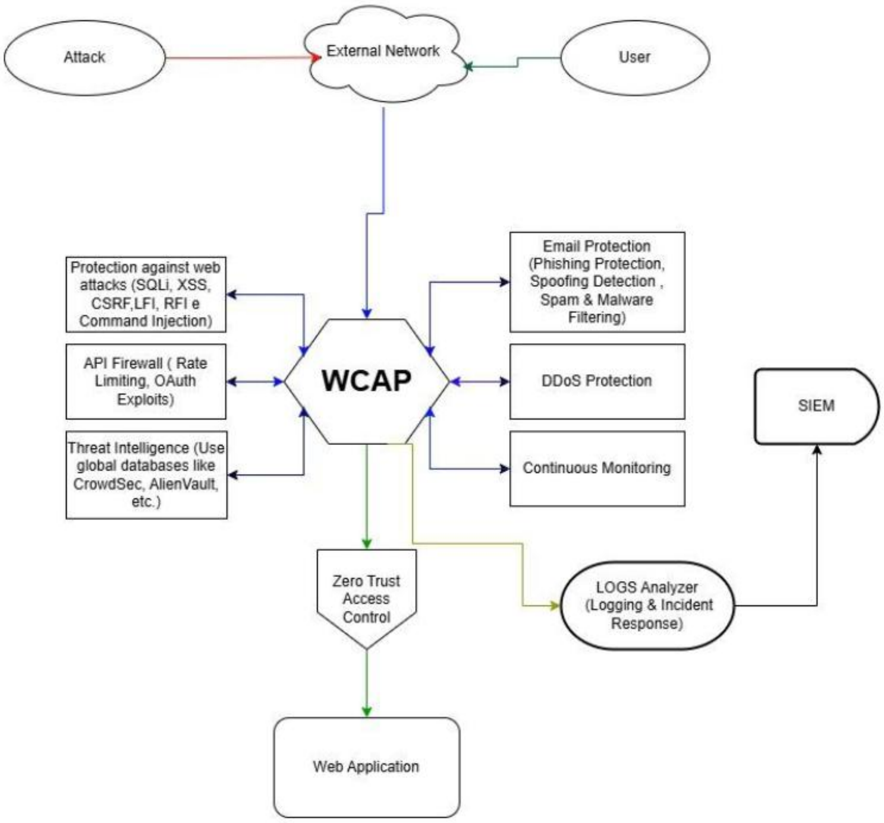
- **Threat Intelligence** (Global threat databases such as CrowdSec, AlienVault, custom or third-party sources)
- **Email Protection** (Phishing Protection, Spoofing Detection, Spam Filtering)
- **DDoS Protection** (Mitigation of volumetric and targeted attacks)
- **Continuous Monitoring and Log Analysis**
- **Zero Trust Access Control** (Continuous validation of identity and permissions)

Optional Expansions:

In addition to these core layers, WCAP-based solutions may include extra modules such as **insider threat prevention**, **AI-driven behavior analysis**, **multi-cloud security**, and **automated incident response**, as long as they follow WCAP's principles of **native protection**, **adaptive context-awareness**, and **efficient orchestration**.

3.2 Architecture Diagram

The WCAP architecture is structured into modular layers that work together to ensure comprehensive protection of web applications. The diagram below illustrates the core components of a WCAP-compliant system, highlighting the native integration between each layer and their collective role in enforcing security, observability, and automated response.


Attack
External Network
User
Protection against web attacks (SQLi, XSS, CSRF,LFI, RFI e Command Injection)
API Firewall (Rate Limiting, OAuth Exploits)
Threat Intelligence (Use global databases like CrowdSec, AlienVault, etc.)
WCAP
Email Protection (Phishing Protection, Spoofing Detection , Spam & Malware Filtering)
DDoS Protection
Continuous Monitoring
SIEM
Zero Trust Access Control
LOGS Analyzer (Logging & Incident Response)
Web Application

4. WCAP Use Cases

4.1 Application in Enterprises and Public Websites

The WCAP concept can be applied across various sectors that require full protection for web applications, ensuring security, compliance, and mitigation of advanced threats. For a solution to be considered WCAP-compliant, it must implement all the minimum security layers or more, ensuring a secure, resilient, and integrated environment. Below are the main sectors that benefit from this model:

E-commerce

E-commerce websites are frequent targets of fraud, DDoS attacks, and exploitation of payment APIs.

A WCAP-compliant model protects online stores by ensuring:

- **Protection against fraud and credential theft** → Integration with Threat Intelligence to detect brute force attacks and malicious login attempts.
- **Security for payment APIs** → Protection against API abuse, OAuth exploitation, and rate limiting to prevent botnet attacks.
- **Defense against DDoS and scraping** → Blocking attempts to extract prices, information, and customer data.
- **Checkout and payment data protection** → Implementation of Zero Trust layers and continuous transaction validation.

Banks and Fintechs

Financial institutions require advanced protection against banking fraud, identity theft, and sophisticated attacks.

A WCAP-compliant solution provides:

- **Phishing and fraud mitigation** → Blocking malicious emails targeting clients and staff.
- **Protection against injection attacks (SQLi) and API exploitation** → Security for banking data and critical interfaces.
- **Zero Trust for login and authentication** → Continuous session validation, anomaly detection, and advanced MFA.
- **Defense against targeted DDoS** → Protection from volumetric attacks aimed at disabling online banking services.

SaaS and Cloud Applications

SaaS platforms and multi-cloud environments require protection for users, data, and exposed APIs.

A WCAP-compliant solution provides:

- **Multi-tenancy protection** → Ensures isolation between users and organizations within the SaaS platform.
- **Security for REST/GraphQL APIs** → Rate limiting, authentication control, and monitoring of suspicious calls.
- **Mitigation of cloud infrastructure attacks** → Integration with Threat Intelligence to detect targeted threats.
- **Zero Trust for administrative access** → Ensures no administrative request is trusted by default.

News and Open Content Sites

News portals and open content sites must ensure public accessibility without compromising security.

A WCAP-compliant solution protects against:

- **Defacement and malicious code injection** → Protection from XSS, CSRF, and code injection.
- **DDoS and scraping** → Blocking attacks aimed at server disruption or content theft.
- **Admin credential protection** → Implementation of Zero Trust and MFA for content management.
- **Security for publishing and distribution APIs** → Control over APIs that send, publish, and share news.

Government and Critical Infrastructure

Government entities and critical infrastructures (energy, telecommunications, healthcare) face high risks of cyberattacks, espionage, and digital sabotage.

WCAP-compliant solutions ensure:

- **Zero Trust for government portals and critical systems** → No request is trusted by default, enforcing continuous authentication and strict access control.
- **Protection of public APIs and services** → Prevention of injection attacks, exploitation of critical endpoints, and data tampering.
- **Continuous monitoring and threat intelligence** → Integration with Threat Intelligence to predict and block targeted attacks.
- **Resilience against state-sponsored and APT attacks** → Detection of malicious patterns and automated response to persistent threats.

- **Defense against DDoS targeting government systems** → Mitigation of attacks aimed at disabling critical services such as voting systems, national databases, and telecom networks.

Healthcare and Hospitals

The healthcare sector depends on data availability and integrity for critical operations, making it a target for data theft and manipulation of medical records.

WCAP-compliant solutions ensure:

- **Zero Trust for access to Electronic Medical Records (EMRs)** → No access should be trusted without strong authentication and behavior analysis.
- **Security for telemedicine APIs and connected medical devices (IoT)** → Continuous monitoring to prevent unauthorized access and attacks on clinical devices.
- **DDoS protection to ensure operational continuity** → Prevention of attacks that could disrupt hospital and clinic operations.
- **Threat intelligence applied to health data** → Continuous analysis of suspicious patterns in requests to medical databases.

Education and Universities

Academic institutions operate dynamic and decentralized environments, making them targets for credential theft, phishing, and exploitation of educational networks.

WCAP-compliant solutions ensure:

- **Zero Trust for students, faculty, and researchers** → Implementation of continuous authentication and access segmentation.
- **Protection against academic data leakage** → Strict access control over research repositories and sensitive data.
- **Security for e-learning platforms** → Prevention of injection attacks and exploitation of online course APIs.
- **DDoS protection to ensure availability of educational platforms** → Monitoring and mitigation of service disruption attempts.

Gaming and Streaming Sector

Online gaming platforms and streaming services are targets of DDoS attacks, API exploitation, and credential theft from gamers and subscribers.

WCAP-compliant solutions provide:

- **Real-time protection against volumetric DDoS attacks** → Monitoring and automatic mitigation of attempts to disrupt gaming and streaming servers.
- **Zero Trust for login and authentication** → Continuous control of suspicious access and prevention of account fraud.

- **Protection of matchmaking and transaction APIs** → Security against manipulation of online games and payment APIs.
- **Continuous monitoring of malicious traffic** → Threat intelligence to detect and block abusive behaviors and automated attacks.

4.2 Zero Trust Applied to WCAP

The concept of Zero Trust within a WCAP-compliant solution ensures that no request, user, or device is trusted by default. It enforces continuous authentication, behavioral analysis, and adaptive security monitoring.

Zero Trust as applied to WCAP establishes a continuous and adaptive security model in which access to web applications, APIs, sensitive data, and administrative panels is constantly validated.

This approach significantly reduces the risk of unauthorized access, lateral movement within the environment, and exploitation of privileged systems—ensuring that only legitimate, verified, and contextually appropriate entities are granted access at any time.

How WCAP Implements Zero Trust

Public Traffic vs. Authenticated Traffic

To ensure efficient access control, WCAP distinguishes between public traffic and authenticated traffic, applying specific policies accordingly:

- **Public Traffic:**
  Any unauthenticated request follows a reputation validation flow, which may include threat intelligence analysis, detection of anomalous traffic, assessment of suspicious IPs, and navigation heuristics.
- **Authenticated Traffic:**
  Any authenticated request undergoes multiple layers of verification, including continuous authentication, user behavior analysis, device reputation assessment, and compliance with established security policies.

This differentiated approach ensures that both public and privileged interactions are handled with the appropriate level of scrutiny, supporting a dynamic and risk-based security posture.

Difference Between Public and Authenticated Traffic in WCAP

Request	WCAP Validation
Anonymous visitor accessing public website	IP reputation, bot detection, behavioral analysis
Authenticated user accessing restricted area	MFA, continuous session analysis, device validation
Call to critical APIs	OAuth authentication, integrity validation, rate limiting
Administrator accessing control panel	MFA, Zero Trust Access Control, location and behavior analysis

Continuous Authentication Policy Enforcement

WCAP requires continuous authentication, meaning that a user or system cannot maintain indefinite access without validation. This can be implemented as follows:

- **Periodic session revalidation** → Access tokens expire in short cycles and require risk-based reauthentication.
- **Dynamic MFA** → When a user accesses from a new location, device, or exhibits suspicious behavior, the system enforces enhanced authentication.
- **Session monitoring** → If an authenticated user demonstrates anomalous behavior (e.g., rapidly accessing multiple accounts), WCAP can trigger a forced re-login or block access entirely.

This dynamic enforcement of authentication ensures ongoing validation of trust, reducing the risk of session hijacking and unauthorized access.

Zero Trust Implementation in WCAP-Compliant Environments

For effective implementation of Zero Trust within WCAP, the following elements must be structured:

- **Identity and Access Management (IAM) Policy** → Establish strict rules for user and device access.
- **Adaptive Authentication** → Apply authentication based on user context, risk levels, and behavioral patterns.
- **Microsegmentation** → Enforce policies ensuring that even authenticated users have access only to what is necessary.
- **Continuous Monitoring and Behavioral Analysis** → Validate user sessions in real time and apply dynamic policies.
- **API and Webhook Protection** → Implement specific rules to prevent unauthorized access to critical endpoints.
- **Integrated Threat Intelligence** → Block access based on known attack patterns, malicious IPs, and API exploitation attempts.

By combining these components, WCAP enables a robust Zero Trust framework that minimizes exposure and ensures that only verified and compliant entities interact with sensitive systems.

When to Apply Zero Trust within WCAP?

Zero Trust should be applied whenever authentication or interaction with sensitive data occurs. Use cases within WCAP include:

- **Administrative Panels** → Protection against session hijacking and brute force attacks.
- **Public and Private APIs** → Prevents data exposure and exploitation by malicious third parties.

- **High-Risk Users** → Enforcement of additional rules for users accessing from suspicious locations or devices.
- **Long and Persistent Sessions** → Enforce periodic renewal and continuous credential validation.

Applying Zero Trust in these scenarios ensures that only trusted, verified entities can access sensitive areas and resources, maintaining the integrity and security of the application environment.

Structuring Zero Trust in WCAP

To correctly implement Zero Trust in a WCAP-compliant solution, a layered security model is required:

Layer 1: Identity and Access

- Mandatory MFA for administrative and critical access.
- Validation of trusted devices and access history.

Layer 2: Continuous Monitoring and Session Analysis

- Use of Machine Learning and AI to detect suspicious access.
- Real-time monitoring of both authenticated and unauthenticated traffic.

Layer 3: Granular Restrictions and Incident Response

- Enforcement of least privilege access policies.
- Automatic detection of lateral movement attempts and insider threats.
- Automated responses such as session termination, IP blocking, and alert notifications.

The implementation of Zero Trust within WCAP ensures that all interactions with web applications and APIs are continuously validated—reducing fraud, unauthorized access, and vulnerabilities.

Organizations that adopt WCAP-compliant solutions with Zero Trust achieve native and adaptive protection, eliminating risks associated with compromised credentials, lateral movement, and session hijacking.

5. Comparison with Traditional Solutions

5.1 Difference Between WCAP and Traditional WAF

Traditional security solutions, such as standalone WAFs, SIEMs, and API firewalls, attempt to mitigate cyber risks but fall short in providing a unified and adaptive approach to web application protection. A WCAP-compliant solution addresses these issues by integrating native protection with advanced security layers, eliminating the weaknesses of fragmented systems.

Why migrate to WCAP-compliant solutions?

The WCAP architecture delivers continuous, integrated, and automated security, whereas traditional solutions often rely on multiple disconnected products—leading to protection gaps and operational challenges.

WCAP vs. Traditional WAF – Feature Comparison

Feature	WCAP	Traditional WAF
API Protection	Yes – Natively protects APIs with rate limiting, authentication, and endpoint security.	No – Only protects HTTP traffic; does not account for REST or GraphQL APIs.
Email Protection	Yes – Integrated with threat intelligence to detect phishing, spoofing, and email-based malware.	No – WAFs do not offer protection against email-borne threats.
Threat Intelligence	Yes – Uses AI and global feeds to anticipate threats before they impact the application.	Limited – Only blocks known attack patterns; lacks predictive analysis.
Zero Trust	Yes – Implements continuous authentication and restriction of untrusted access.	No – WAFs do not enforce ongoing identity verification.
Response Orchestration	Yes – Automates blocking, incident response, and attack containment.	No – Only generates alerts; does not automate mitigation.
Advanced DDoS Protection	Yes – Mitigates volumetric and Layer 7 attacks with adaptive intelligence.	Limited – Only blocks basic DDoS patterns.
Behavioral Analysis and Automated Response	Yes – Monitors user and traffic behavior to identify advanced threats.	No – WAFs analyze only individual requests without context.
Continuous Monitoring and Telemetry	Yes – Includes detailed real-time logging of events, traffic, and attack attempts.	Limited – May generate logs but lacks deep and continuous analysis.
Protection Against OAuth API Exploits and JWT Tokens	Yes – Continuously validates misuse of credentials and token manipulation.	No – Lacks intelligence to detect advanced authentication exploits.

Rationale for Building Solutions with WCAP

Reduction in Operational Complexity

Traditional solutions require multiple products to cover different attack vectors (e.g., WAF + API firewall + email protection tools). This leads to complex integrations, high costs, and security blind spots. A WCAP-compliant approach eliminates this fragmentation by providing a unified protection model.

Adaptive and Intelligent Security

While a traditional WAF relies on fixed rules and known threat signatures, WCAP applies predictive intelligence through machine learning and behavioral analysis to anticipate attacks. This results in reduced dependence on static rules and a greater ability to detect novel and previously unseen threats.

Native Implementation of Zero Trust

Most traditional WAFs do not enforce Zero Trust, leaving vulnerabilities in internal access and authenticated traffic. WCAP-compliant solutions implement continuous authentication, dynamic access restrictions, and strict segmentation—ensuring that no identity or device is trusted by default.

Automated Response and Remediation

While WAFs can generate alerts, they often fail to proactively block threats. WCAP is designed to automatically respond to incidents by blocking malicious traffic and isolating threats in real time.

Greater Efficiency in API Protection

API traffic is critical for modern applications, yet traditional WAFs lack the intelligence to protect API calls from abuse and targeted attacks. WCAP-compliant solutions include a native API firewall, protecting OAuth authentication, JWT tokens, and preventing endpoint abuse.

By adopting WCAP-compliant solutions, organizations can reduce operational complexity, improve incident response, and eliminate vulnerabilities left behind by traditional tools. Unlike the fragmented model of WAF plus additional firewalls, WCAP integrates comprehensive protection, automation, and adaptive intelligence—becoming the new standard in web application security.

WCAP Implementation

Objective:
Provide technical guidelines for organizations to develop solutions based on the WCAP model, ensuring compliance with its core principles. This section outlines the minimum requirements, recommended frameworks, and best practices for building WCAP-compliant systems, enabling developers, security architects, and technology providers to implement the model effectively.

Development Guidelines

To be WCAP-compliant, a solution must meet a set of minimum requirements and offer expansion capabilities, ensuring continuous security and scalability. Below are the essential development guidelines:

A WCAP solution must include all fundamental layers to be considered WCAP-compliant.

Essential Requirements

To be considered WCAP-compliant, a solution must meet the following core requirements:

- **Web Application Protection** → Implementation of a Web Application Firewall (WAF) to mitigate attacks such as SQL Injection, XSS, CSRF, LFI/RFI, and exploitation of vulnerabilities in HTTP headers.
- **API Protection** → Native API firewall with rate limiting, OAuth-based authentication, API traffic monitoring, and endpoint attack prevention.
- **Integrated Threat Intelligence** → Capability to utilize global threat feeds (e.g., CrowdSec, AlienVault), machine learning, and predictive analysis to anticipate attacks.
- **Advanced DDoS Protection** → Implementation of mitigation layers against volumetric attacks (Layer 3/4) and application-layer attacks (Layer 7).
- **Zero Trust Access Control** → Enforcement of continuous access control, adaptive authentication, and strict permission segmentation.
- **Incident Monitoring and Response** → Detailed log collection, event correlation, automated response, and SIEM integration.
- **Protection Against Phishing and Malicious Emails** → Email traffic monitoring to detect attacks such as spoofing, phishing, and Business Email Compromise (BEC).
- **Security Orchestration and Automation** → Adoption of automated response playbooks, real-time mitigation policies, and behavioral analysis.

Development Structure

Web Application Protection

OWASP Guidelines:

- Apply the controls defined in the OWASP Top 10 to mitigate vulnerabilities such as SQL Injection (A03:2021), XSS (A07:2021), CSRF, and broken authentication (A07:2021).
- Implement security headers in accordance with the OWASP Security Headers Project, including Content Security Policy (CSP), Strict-Transport-Security (HSTS), and X-Frame-Options.
- For APIs, follow the OWASP API Security Top 10, protecting endpoints against weak authentication, data exposure, and authorization failures.

MITRE ATT&CK:

- Map tactics and techniques from the MITRE ATT&CK framework, such as:
  - T1190 – Exploit Public-Facing Application
  - T1071.001 – Command and Control over HTTP

  - T1133 – External Remote Services
- Integrate automation to enable active response to attacks based on MITRE ATT&CK technique patterns.

CIS Controls:

- Mandatory application of:
  - CIS Control 3 – Web Application and Email System Protection
  - CIS Control 11 – Secure Configuration for Network Devices (Web Defense)
- Implement continuous monitoring as outlined in CIS Control 6 – Audit Log Management.

Zero Trust (NIST SP 800-207):

- Ensure that all requests undergo strict authentication and continuous identity validation, eliminating implicit trust.
- Apply segmentation to prevent lateral movement and restrict application access strictly to what is necessary.

API Protection

OWASP:

- Follow the recommendations from the OWASP API Security Top 10, including:
  - Protection against API Injection (API3:2023)
  - Prevention of Excessive Data Exposure (API2:2023)
- Apply OAuth 2.0 and OpenID Connect for robust client and user authentication.

MITRE ATT&CK:

- Monitor for malicious patterns based on:
  - T1190 – Exploit Public-Facing Application
  - T1071.001 – Command and Control over HTTP
- Apply API traffic analysis to detect anomalous behavior, such as repetitive calls or endpoint enumeration attempts.

Zero Trust:

- No API should be accessible without continuous authentication.
- Enforce dynamic rate limiting and permission restrictions based on roles and security policies.

Integrated Threat Intelligence

MITRE ATT&CK:

- T1087.002 – User Account Enumeration (Cloud): Detect reconnaissance attempts targeting applications and APIs.
- T1190 – Exploit Public-Facing Application: Map exploitation patterns based on threat intelligence sources.
- T1071.001 – Command and Control via HTTP: Monitor suspicious traffic that mimics C2 communications.
- T1203 – Exploitation of Client Software: Identify attacks exploiting known software vulnerabilities.

CIS Controls:

- CIS Control 6 – Audit Log Management: Mandatory SIEM implementation and event correlation for early detection of emerging attacks.
- CIS Control 7 – Malware Defenses: Integration with threat intelligence feeds for proactive blocking of suspicious files and malicious domains.

Zero Trust:

- Threat Intelligence Feeds: Continuous integration with global databases of malicious IPs, domain blocklists, and attack signatures to enable real-time blocking.
- Adaptive Trust Policies: Dynamic enforcement of access controls that adjust permissions and blocks based on contextual intelligence and risk analysis.

Advanced DDoS Protection

OWASP:

- OWASP API Security Top 10 (API4:2023 – Lack of Rate Limiting): Enforce rate limiting to prevent abuse through malicious requests.
- OWASP Application Security Verification Standard (ASVS): Implement controls to validate legitimate traffic and mitigate massive packet injection attacks.

MITRE ATT&CK:

- T1498 – Denial of Service (DoS): Monitor and mitigate attacks that exploit computational resources to degrade system performance.
- T1499 – Distributed Denial of Service (DDoS): Detect and respond to volumetric attacks and service exhaustion attempts.
- T1498.001 – Network-Based DoS: Protect against amplification attacks and exploitation of insecure protocols.
- T1498.002 – Application-Layer DoS: Identify HTTP Flood attacks and targeted Layer 7 threats.

CIS Controls:

- CIS Control 12 – Network Infrastructure Management: Apply filtering and Deep Packet Inspection (DPI) to mitigate Layer 3–7 attacks.
- CIS Control 13 – Boundary Defense: Implement automated mitigation systems to detect traffic anomalies and block real-time attacks.

Zero Trust:

- IP Reputation and Continuous Monitoring: No request should be processed without evaluation of IP reputation, ASN, and threat intelligence correlation.
- Adaptive Authentication: Enforce strong authentication (MFA, advanced captchas) for suspicious traffic or anomalous requests.

Zero Trust Access Control

Zero Trust (NIST SP 800-207):

- Continuous Authentication & Least Privilege Access: Each request must be dynamically authenticated based on behavioral analysis, identity validation, and associated risk.
- Microsegmentation and Granular Policies: No user or service should be granted access without explicit authorization to the specific resource.

MITRE ATT&CK:

- T1078 – Valid Accounts: Continuous monitoring of suspicious login attempts, including access from unrecognized locations or devices.
- T1566.001 – Phishing with Malicious Links: Enforcement of policies to prevent credential theft and detection of login attempts using leaked credentials.
- T1021.001 – Remote Desktop Protocol (RDP): Blocking unauthorized access to administrative services and controlling sessions of privileged users.

CIS Controls:

- CIS Control 16 – Account Security and Password Management: Enforcement of strong authentication policies, including MFA, secure passwords, and adaptive tokens.
- CIS Control 5 – Account Management of Privileged Users: Strict restriction on administrative accounts and continuous monitoring of elevated sessions.

Incident Monitoring and Response

OWASP:

- OWASP Application Security Verification Standard (ASVS): Apply verification requirements for security log collection and analysis, anomaly detection, and response to suspicious events.

- OWASP Top 10 (A09:2021 – Security Logging and Monitoring Failures): Ensure that all critical events are properly logged and analyzed for rapid response.

MITRE ATT&CK:

- T1057 – Process Discovery: Monitor processes to detect suspicious behavior in web servers and applications.
- T1071.001 – Command and Control over HTTPS: Identify C2 traffic disguised as legitimate HTTPS connections.
- T1020 – Data Exfiltration over Network: Monitor for attempts to exfiltrate sensitive data.
- T1562.004 – Indicator Removal from Logs: Detect and block attempts to tamper with or delete critical logs.

CIS Controls:

- CIS Control 6 – Audit Log Management: Mandatory implementation of SIEMs and event correlation for real-time security analysis.
- CIS Control 19 – Incident Response Management: Structured procedures for quick response to security incidents.
- CIS Control 8 – Logging and Audit Trails: Secure storage and continuous analysis of critical logs for forensic tracing.

Zero Trust:

- Continuous Session Monitoring: Detection of anomalous access patterns and suspicious behavior.
- Automated Response: Immediate actions such as session isolation, termination of suspicious connections, and incident alerting.
- SOAR Integration: Orchestration of automated responses and real-time threat mitigation.

Protection Against Phishing and Malicious Emails

OWASP:

- OWASP Phishing Defense Cheat Sheet: Implement phishing protection policies, including reputation-based filtering and analysis of suspicious email patterns.
- OWASP Top 10 (A04:2021 – Insecure Design): Apply controls to prevent manipulation of email flows and injection of malicious data.

MITRE ATT&CK:

- T1566.001 – Phishing with Malicious Links: Detection of emails containing malicious URLs or social engineering tactics.
- T1566.002 – Phishing with Malicious Attachments: Identification and analysis of email attachments that exploit software vulnerabilities.

- T1583.003 – Domain Registration for Social Engineering: Monitoring of newly registered domains used for phishing campaigns.
- T1204.001 – Execution via Email Attachment: Detection of files or macros that exploit vulnerabilities in email clients.

CIS Controls:

- CIS Control 3 – Protection Against Social Engineering and Phishing Attacks: Implement advanced content filters to detect phishing attempts.
- CIS Control 9 – Email and Web Browser Protections: Enforce SPF, DKIM, and DMARC to validate senders and prevent spoofing.
- CIS Control 13 – Network Segmentation: Isolate malicious emails for quarantine and further analysis.

Security Orchestration and Automation

OWASP:

- OWASP Automated Threats to Web Applications (OAT): Implement detection and automated response mechanisms against web threats.
- OWASP Application Security Verification Standard (ASVS): Apply controls for continuous authentication, automated mitigation, and adaptive incident response.

MITRE ATT&CK:

- T1078 – Valid Accounts: Real-time detection of compromised credentials and automated response.
- T1562.001 – Disable or Modify Tools: Monitor and block attempts to disable firewalls, WAFs, and security agents.
- T1489 – Service Stop: Prevent attackers from shutting down critical servers.

CIS Controls:

- CIS Control 18 – Incident Response and Management Automation: Implement SOAR platforms for automated incident response.
- CIS Control 14 – Controlled Access Based on Need to Know: Automatically adjust user privileges based on behavior and risk.
- CIS Control 16 – Account Monitoring and Control: Automate revocation of leaked credentials, block suspicious accounts, and enforce risk-based MFA.

Zero Trust:

- Behavior-Based Automated Response: Actions such as dynamic IP blocking, session revocation, and reauthentication enforcement.
- AI-Driven Anomaly Detection: Use of Machine Learning to predict threats before execution.

- False Positive Reduction: Adaptive rule tuning based on the history of confirmed threats.

Each WCAP protection layer must be built upon internationally recognized best practices and frameworks, ensuring robust and adaptive security.

Building WCAP-compliant solutions requires a modular, integrated, and industry-aligned approach. Organizations that adopt this model ensure advanced protection, security automation, and resilience against modern threats.

SIEM and Log Integration

Log Processing Flow

Logs must be generated from multiple WCAP layers, including:

- Application Firewall (WAF/WCAP): Captures SQL Injection, XSS, CSRF, LFI/RFI attempts, and authentication attacks.
- API Protection: Logs access to critical endpoints, Rate Limit Bypass attempts, OAuth abuses, and JWT exploits.
- Session and Authentication Monitoring: Logs suspicious login attempts, invalid MFA, and compromised credentials.
- DDoS Protection: Generates metrics on anomalous requests, volumetric traffic, TCP SYN floods, HTTP floods, and response time anomalies.
- Email and Phishing Protection: Captures phishing attempts, spoofing, suspicious attachments, and social engineering attacks.
- Orchestration and Automation: Logs automated actions performed by SOAR, including blocks, incident responses, and threat containment.

Log Transmission to SIEM

Collected logs must be securely transmitted to a centralized SIEM. Common transmission methods include:

- Syslog (UDP/TCP 514): Used for direct delivery to SIEMs like Splunk, QRadar, Wazuh.
- Log APIs (Webhook, RESTful API): Real-time transmission to cloud-based SIEM platforms like Elastic Security and AWS GuardDuty.
- Log Agents (Filebeat, Fluentd, Wazuh Agent): Captures local logs and sends them for centralized analysis.
- Kafka / Message Queues: For high-volume environments, logs are sent to a message broker for scalable processing.

Processing and Enrichment

At this stage, logs must be normalized, analyzed, and correlated with threat intelligence:

- Parsing and Normalization: Converts raw logs into structured formats (e.g., JSON, ECS – Elastic Common Schema).
- **Threat Intelligence Enrichment:**
  - OpenCTI, AlienVault OTX, CrowdSec: Used to check IPs, domains, and malicious hashes.
  - IP and ASN Reputation Analysis: Enables dynamic blocking of suspicious traffic.
  - Credential Breach Cross-Check: Identifies compromised users using databases like *Have I Been Pwned*.
- **Anomaly Behavior Detection (Machine Learning):**
  - Users accessing from different countries in short intervals (geographic impossibility).
  - Sudden spikes in unusual HTTP request patterns.
  - Multiple authentication attempts without successful MFA validation.

POCs added in attached GitHub repository.