

Overview

Web applications have become the backbone of modern business operations, serving as the primary interface between organisations and their customers, partners, and employees. This pivotal role, coupled with the rapid pace of development and deployment, creates a constantly shifting landscape that requires vigilant security measures to protect against evolving web threats.

Cynode designed one of the industry's most comprehensive web application detection and response services, addressing this requirement by offering threat detection, analysis, and mitigation across all key web attack surfaces and security controls, including IaaS Web Servers, PaaS Web Platforms, Cloud Platforms, API Gateways, Web Application Firewalls, and IDS/IPS Security Solutions.

Benefits

Lowered Risk Across the Whole Web Application Estate

Offering a detection and response capabilities that encompasses web platforms and security tools together, attacks targeting web applications are consistently eliminated.

Streamlined Operations Between Devops and Security Teams

Lowers operational cost and risk by enhances collaboration between security and development teams, promoting secure coding practices and empowering security analysts with actionable threat intelligence.

Reduced Alert Fatigue and Noise

With Cynode's ability to correlate alerts from various security tools and apply behavioural anomaly detection, the service drastically reduces the number of false positives, improving operational efficiency and saving time.

Lowered Operational Cost

By consolidating functions such as exposure analysis, and real-time detection into a single platform and assigning complex operations to the Cynode team, operational expenditures (OPEX) are lowered.

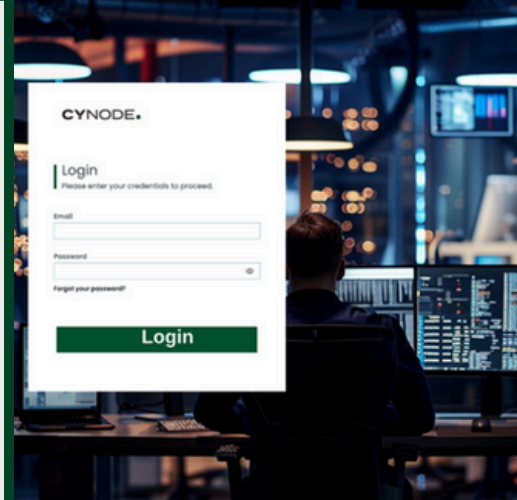
Quicker Access to Talent

By using this service, organisations gain access to web application security experts who are typically difficult to find and recruit.

Key Features

Comprehensive Attack Coverage

The service focuses on the OWASP Top 10 Web Application Security Risks and responds to complex threats unique to web environments, such as bot-driven attacks, automated exploitation, and advanced persistent threats (APTs). It detects and responds to attack types such as injection attacks, authentication bypasses, session hijacking, and cross-site scripting targeting web applications, APIs, and other public-facing assets, ensuring robust protection against evolving cyber threats.



Key Facts

- According to a 2024 study by Okta, the average large organisation (1,000+ employees) uses 187 web applications, while smaller companies (1-250 employees) use an average of 89 apps. This proliferation of web applications significantly expands the attack surface for potential cyber threats. Source: Okta Businesses at Work 2024 Report
- In 2023, web application attacks accounted for over 70% of all data breaches, highlighting their prevalence in cybersecurity threats. Source: Verizon 2023 Data Breach Investigations Report
- The average cost of a web application attack for large enterprises reached \$3.86 million in 2024. Source: IBM Cost of a Data Breach Report 2024
- 42% of organisations reported insufficient resources to adequately secure their web applications against emerging threats. Source: SANS Institute 2024 State of Application Security Survey

Single Point of Visibility for All Web-Based Security Events

Cynode MDR for Web Applications service tackles both general and sophisticated attack types targeting web applications, providing a single point of visibility for all web-based hosting and security events. Cynode's Workspace Platform offers clients a dashboard with key metrics such as:

- Volume of detected threats and incident types
- Threat classifications according to OWASP Top 10
- Affected applications and assets
- MITRE ATT&CK heat map for web-related threats

Unified Detection Across Multiple Web Security Layers

Cynode integrates logs and alerts from various sources, centralising and streamlining web threat visibility.

- IaaS Web Servers (e.g., Amazon EC2, Microsoft Azure Virtual Machines)
- PaaS Web Platforms (e.g., Azure App Service, Heroku, Google App Engine)
- API Gateways (e.g., Amazon API Gateway, Azure API Management)
- Web Application Firewalls (e.g., F5, Imperva, Cloudflare WAF, AWS WAF)
- IDS/IPS Security Solutions (e.g., Palo Alto Networks, Fortinet, Checkpoint, Trellix, Snort, Suricata)

Tailored Detection for Web Threats

Adapts and improves the security posture of complex web application environments, including multi-cloud deployments, microservices architectures, and CI/CD pipelines. The service's detection rules are customised for each organisation's application hosting platforms and security solutions. Cynode categorises these rules based on the MITRE ATT&CK and OWASP Top 10 frameworks.

Specialised Web Threat Intelligence

Cynode combines industry-specific threat intelligence with behaviour-based detection to identify high-risk threats to web applications. This includes protection against new attack methods targeting APIs and customer-facing applications.

Continuous Exposure and Configuration Management

Using the Ultima Exposure Management Platform, Cynode continuously assesses exposure by identifying misconfigurations, weak access controls, and policy deviations that could increase vulnerability to emerging web-based threats.

Real-Time Anomaly Detection

Cynode leverages behavioural analytics to detect abnormal activities, such as high-volume bot traffic, unusual API access patterns, and repetitive login attempts, signalling credential-stuffing or brute-force attacks.

Proactive Mitigation of Targeted Attacks and Random Scans

The Cynode MDR service proactively identifies and mitigates vulnerabilities exposed to daily random scans and targeted attacks.

Real-Time Detection and Immediate Response to Threats

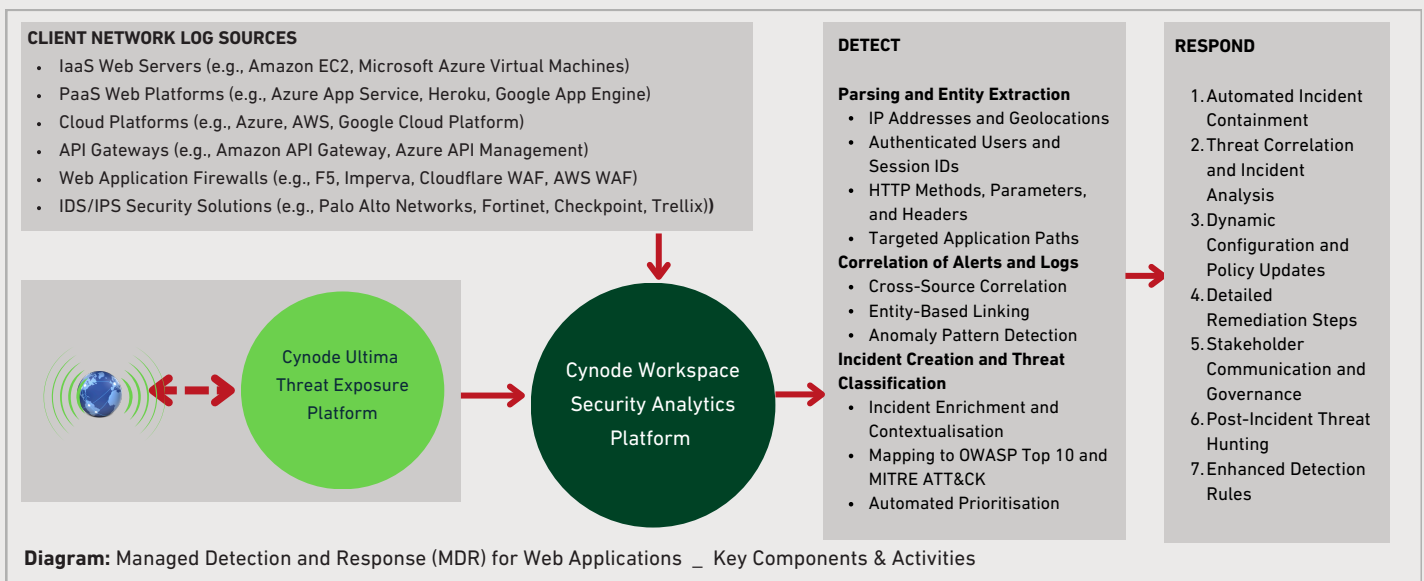
Continuous monitoring prevents threats from lingering undetected, significantly reducing the chances of successful exploitation. The immediate threat mitigation lowers the risk of data breaches, service disruptions, and reputational damage to the organisation.

Problems Addressed








- Current MDR services in the market lack a specific and comprehensive focus on web applications, failing to encompass both web platforms and security tools adequately.
- The proliferation of multi-cloud environments, microservices, and CI/CD practices increases security challenges, requiring specialised knowledge and coordination between development and security teams.
- Fragmented security solutions generate numerous signals without a unified framework, complicating threat monitoring and response.
- Web applications face daily exposure to both targeted attacks and automated scans. The combination of these random scans and targeted attacks significantly increases the likelihood of a successful breach. The sheer volume and frequency of these scans create a constant barrage of noise in protection and detection tools.
- Many organisations lack in-house expertise for comprehensive web application security strategies.
- Managing multiple security products leads to high CAPEX and OPEX, as organisations invest in integration, management, and maintenance of disparate solutions.

How It Works

Cynode's WebApp Exposure Detection and Response service operates through a comprehensive process of detection and response. In the detection phase, the system collects and analyses logs from multiple sources including WAF solutions, IDS/IPS systems, behavioural anomaly detection tools, and web hosting platforms. These logs are parsed to extract key entities such as IP addresses, user sessions, and HTTP request details. The Workspace Platform then correlates these entities across different sources, transforming isolated alerts into actionable incidents. Incidents are enriched with contextual data, mapped to OWASP Top 10 risks and MITRE ATT&CK tactics, and prioritised based on severity. In the response phase, the platform orchestrates automated containment actions, performs in-depth incident analysis, updates security configurations, and provides detailed remediation steps. This process is complemented by stakeholder communication, post-incident threat hunting, and continuous refinement of detection rules, ensuring a robust and adaptive defence against web application threats.



OTHER CYNODE MDR SERVICES

-  Managed Detection and Response for Endpoint
-  Managed Detection and Response for Microsoft Defender
-  Managed Cloud Apps & Shadow IT
-  Managed Detection and Response for Cloud
-  Managed Phishing Detection and Response
-  Managed Detection and Response for Identity Protection
-  Managed Business Email Compromise Detection and Response