Innovative: International Multi-disciplinary Journal of Applied Technology
(ISSN 2995-486X) VOLUME 04 ISSUE 09, 2026

# RISK-BASED OPTIMIZATION OF WEB APPLICATION FIREWALL POLICIES USING SIEM-DRIVEN LOG ANALYTICS IN DATA CENTER SECURITY

**Ashurov Laziz Shoymardonovich**
Inha University in Tashkent
E-mail: ashurovlaziz@gmail.com
ORCID: https://orcid.org/0009-0008-1899-5241

**Abstract:**

This article examines a risk-based approach to optimizing Web Application Firewall (WAF) policies through SIEM-driven log analytics in data center security environments. The study aims to develop a methodological framework for improving WAF rule effectiveness by correlating web traffic events, security logs, detected anomalies, and risk indicators collected through Security Information and Event Management systems. The proposed approach focuses on reducing false positives, identifying obsolete or overly permissive rules, prioritizing high-risk attack patterns, and adapting WAF policies to dynamically changing threat conditions. The research is based on the analysis of WAF event logs, SIEM correlation mechanisms, risk scoring principles, and policy optimization procedures. Particular attention is paid to the integration of log analytics with rule tuning, event prioritization, and incident response processes. The study shows that risk-based policy management can improve the precision of web application protection by enabling security teams to distinguish between low-impact anomalies and critical attack vectors. The proposed framework also supports continuous monitoring and iterative adjustment of WAF rules based on threat severity, asset criticality, and observed attack behavior. The results indicate that combining SIEM analytics with WAF policy optimization can strengthen data center cybersecurity, improve incident detection quality, and support more efficient security resource allocation.

**Keywords:** Web Application Firewall, WAF policy optimization, SIEM, log analytics, risk-based security, data center security, cybersecurity, threat detection, incident management, rule tuning.

## Introduction

The increasing complexity of modern data center infrastructures has significantly expanded the attack surface of web-based services and applications. Web applications are continuously exposed to threats such as SQL injection, cross-site scripting, command injection, path traversal, automated scanning, credential attacks, and application-layer denial-of-service attempts [1]. In this context, Web Application Firewalls (WAFs) have become an important security control for filtering malicious HTTP/HTTPS traffic and enforcing application-layer security policies.

However, the effectiveness of a WAF largely depends on the quality of its rule configuration and continuous policy maintenance [2], [3]. Static or poorly tuned rules may generate a high number of false positives, block legitimate user requests, fail to detect new attack patterns, or leave unnecessary exceptions within the security policy [4]. A high base rate of benign traffic makes this problem structural rather than incidental, since even a low false-positive probability produces a large absolute number of spurious alerts [5]. As the volume of web traffic and the number of protected applications increase, manual rule adjustment becomes increasingly difficult and may lead to inefficient security management.

Security Information and Event Management (SIEM) systems provide additional capabilities by collecting, normalizing, correlating, and analyzing security events from multiple sources [6]. In a data center environment, SIEM platforms can aggregate WAF logs together with operating system events, application logs, authentication records, intrusion detection alerts, network telemetry, and other security data. This integrated view makes it possible to assess web attacks not only as isolated WAF events, but also as part of a broader security context. Studies of security operations centres identify precisely this aggregation and triage function, together with alert overload, as central operational challenges [7].

A risk-based approach can further improve WAF policy management by prioritizing events and rules according to their potential impact. Instead of treating all detected anomalies equally, risk-based optimization considers factors such as attack severity, frequency, asset criticality, vulnerability exposure, event confidence, source behavior, and possible business consequences [8], [9]. This enables security teams to focus on rules associated with the most significant threats while reducing unnecessary blocking and alert overload.

The combination of SIEM-driven log analytics and risk-based WAF policy optimization therefore represents a promising approach to adaptive web application protection. Through continuous analysis of event data, security teams can identify ineffective rules, detect repeated attack patterns, recognize abnormal behavior, and adjust protection policies according to the actual threat environment.

The objective of this study is to develop and substantiate a risk-based framework for optimizing Web Application Firewall policies using SIEM-driven log analytics in data center security. The study focuses on the processes of event correlation, risk scoring, rule prioritization, false-positive reduction, and continuous WAF policy adjustment in order to improve the accuracy and operational efficiency of web application security.

## Materials And Methods

The study employed a risk-oriented methodological framework combining Web Application Firewall event analysis, SIEM-based log correlation, threat prioritization, and iterative WAF rule optimization. The methodological design was structured to evaluate how security event data can be transformed into actionable policy adjustments within a data center environment [10].

The analyzed security architecture consisted of four logical layers: protected web applications, the WAF layer, centralized log collection, and the SIEM analytics layer. The WAF was considered the primary application-layer filtering mechanism, while the SIEM platform served as the central component for event normalization, correlation, risk assessment, and incident prioritization [11].

Security data were obtained from several categories of sources: WAF access and security logs, web server logs, application logs, authentication records, operating system events, intrusion detection alerts, and network security telemetry [6]. These data sources were selected because isolated WAF alerts may not provide sufficient contextual information for determining the actual severity of an

event. Correlation with additional log sources enables a more accurate assessment of attack intent and potential impact.

Before analysis, raw log records were normalized into a unified event structure in accordance with established log-management practice [6]. The principal attributes included source IP address, destination host, timestamp, HTTP method, requested URI, response status code, WAF rule identifier, attack category, severity level, user-agent information, authentication status, and frequency of repeated events. Duplicate and technically insignificant events were filtered to reduce noise in the analytical dataset.

A risk score was assigned to each security event using a multi-factor assessment model in which severity and vulnerability exposure follow standard vulnerability-scoring practice [12] and asset criticality follows established risk-assessment guidance [8]. The proposed score can be represented as:

$$R = w_1S + w_2A + w_3F + w_4C + w_5V$$

**Table 1. Parameters of the multi-factor risk assessment model**

| Symbol | Risk factor | Role in the model |
|---|---|---|
| R | Overall event risk score | Aggregated value used for security-event prioritization. |
| S | Attack severity | Represents the severity of the detected attack. |
| A | Asset criticality | Reflects the importance of the targeted asset. |
| F | Event frequency | Captures recurrence of similar security events. |
| C | Detection confidence | Represents confidence in the detection result. |
| V | Vulnerability exposure | Reflects the exposure level of the protected application. |
| $w_1 \ldots w_5$ | Weighting coefficients | Adjust the contribution of each factor to data-center security priorities. |

For practical interpretation, events were grouped into low-, medium-, high-, and critical-risk categories. High- and critical-risk events received priority during WAF rule review and incident investigation, whereas repeated low-risk events were primarily analyzed as potential false positives or indicators of unnecessarily restrictive rules.

The WAF policy optimization process consisted of several sequential stages. First, frequently triggered rules were identified through SIEM queries and statistical aggregation. Second, these rules were correlated with application behavior and additional security logs. Third, rules associated with excessive false-positive rates, obsolete signatures, redundant conditions, or insufficient coverage were selected for review. Fourth, rule actions were adjusted by modifying thresholds, exception lists, request patterns, or severity assignments [4].

Special attention was given to distinguishing between malicious traffic and legitimate application behavior, a long-standing difficulty in the detection of web-based attacks [13]. A rule was not considered ineffective solely because it produced a high number of alerts. Instead, its effectiveness was evaluated in relation to the proportion of confirmed malicious events, false positives, protected asset criticality, and frequency of repeated attack attempts.

The proposed optimization cycle can be expressed as:

log collection → normalization → SIEM correlation → risk scoring → rule evaluation → WAF policy adjustment → monitoring → re-evaluation.

This closed-loop process supports continuous policy adaptation rather than one-time configuration.
The effectiveness of the optimization methodology was planned to be assessed through the following indicators: false-positive rate, true-positive detection rate, number of redundant alerts, number of high-risk events correctly prioritized, average incident triage time, and the proportion of WAF rules requiring modification [5], [11].

**Table 2. Indicators for evaluating WAF policy optimization**

| Evaluation indicator | Interpretation | Desired effect |
|---|---|---|
| False-positive rate | Benign events incorrectly flagged by WAF rules. | Decrease |
| True-positive detection rate | Correct identification of malicious activity. | Increase |
| Number of redundant alerts | Repeated or overlapping alerts with limited analytical value. | Decrease |
| High-risk events correctly prioritized | Events ranked according to contextual risk. | Increase |
| Average incident triage time | Time required to classify and prioritize a security event. | Decrease |
| WAF rules requiring modification | Rules selected for tuning, consolidation, or review. | Measures optimization scope |

To ensure reproducibility, the evaluation should be conducted over defined observation periods before and after policy optimization. However, quantitative values such as the number of analyzed events, duration of monitoring, protected applications, and exact percentage changes should be reported only on the basis of real experimental data obtained from the target data center environment.

**Results**

The proposed risk-based optimization framework demonstrated that WAF policy management can be significantly improved when rule evaluation is based not only on isolated firewall alerts but also on correlated SIEM data and contextual risk indicators. The analytical results indicate that the most effective policy decisions are obtained when attack severity, asset criticality, event recurrence, detection confidence, and application vulnerability are considered together.

The first important result is the possibility of identifying high-noise WAF rules. SIEM-based aggregation makes it possible to determine which rules generate the largest number of alerts and whether these alerts correspond to confirmed malicious activity. Rules with frequent triggering but low contextual risk can be classified as candidates for tuning, threshold adjustment, or exception management [4].

The second result concerns the prioritization of security events. Risk scoring enables WAF alerts to be divided into low-, medium-, high-, and critical-risk categories. This classification reduces the operational burden on security teams by directing attention toward events that combine strong attack indicators with high-value assets or known vulnerabilities. As a result, security analysis becomes more focused and incident triage can be organized according to actual threat relevance [8].

Another important finding is that SIEM correlation improves the interpretation of WAF events. For example, a single blocked HTTP request may represent a low-priority event when analyzed independently. However, when the same source is associated with repeated authentication failures, reconnaissance activity, or other suspicious network events, the overall risk level increases, since these observations correspond to successive stages of a single adversary behaviour sequence [14]. Thus, contextual correlation provides a more reliable basis for policy optimization than WAF log

analysis alone.

The proposed approach also supports the detection of redundant or obsolete rules. If multiple rules repeatedly identify the same traffic pattern or if a rule no longer corresponds to the current application architecture, SIEM-driven analysis can reveal unnecessary overlap. Removing or consolidating such rules can simplify WAF policy structure and reduce administrative complexity.

A further result is the establishment of a continuous feedback loop between security monitoring and policy adjustment. Instead of treating WAF configuration as a static security task, the proposed framework supports periodic reassessment of rules based on current attack behavior, newly identified vulnerabilities, and changes in application usage patterns [9], [15].

From a methodological perspective, the results can be summarized through four main optimization outcomes: reduction of false-positive alerts, improved prioritization of high-risk incidents, identification of ineffective or redundant rules, and increased adaptability of WAF policies to changing threat conditions.

**Table 3. Analytical outcomes of the proposed optimization framework**

| Analytical outcome | Supporting mechanism | Expected operational effect |
|---|---|---|
| Reduction of false-positive alerts | SIEM correlation and contextual validation of WAF events. | Lower alert noise and fewer unnecessary investigations. |
| Improved prioritization of high-risk incidents | Risk scoring based on severity, asset criticality, recurrence, confidence, and exposure. | Focus on events with greater potential impact. |
| Identification of ineffective or redundant rules | Aggregation of frequently triggered rules and comparison with application behavior. | Simpler and more maintainable WAF policy structure. |
| Greater policy adaptability | Closed-loop monitoring, reassessment, and iterative rule adjustment. | Better response to changing threats and application conditions. |

Since the present study focuses on framework development, these outcomes represent analytical findings rather than statistically validated experimental results. Quantitative indicators such as false-positive reduction percentage, detection accuracy, incident response time, and policy efficiency should be calculated in future experimental validation using real data center logs and controlled before-and-after measurements.

## Discussion

The findings indicate that risk-based optimization of WAF policies becomes more effective when security decisions are based on correlated event context rather than on individual firewall alerts. In traditional configurations, WAF rules are often managed through static thresholds and predefined signatures. Although this approach provides baseline protection, it may produce excessive alerts, create unnecessary blocking, and increase the workload of security analysts. The integration of SIEM-driven log analytics enables WAF events to be interpreted within a broader security context.

A key advantage of the proposed framework is the combination of technical detection indicators with contextual risk factors. Attack severity alone is insufficient for accurate prioritization because the same attack pattern may have different consequences depending on the importance of the target system, its vulnerability status, and the recurrence of suspicious activity. Therefore, the inclusion of asset criticality, event frequency, detection confidence, and vulnerability exposure provides a more balanced basis for risk assessment [8], [12].

The results also highlight the importance of false-positive management. A WAF policy that is

excessively restrictive may negatively affect legitimate application traffic, while overly permissive rules may increase exposure to attacks. SIEM-based analysis allows analysts to distinguish between repeated benign patterns and truly malicious behavior by correlating WAF events with authentication logs, application events, network telemetry, and other security indicators. This supports more precise rule tuning and reduces unnecessary alerts [4], [5].

Another important aspect is policy adaptability. Data center environments are dynamic: applications change, new services are deployed, vulnerabilities are discovered, and attack techniques evolve. For this reason, WAF policy optimization should not be treated as a one-time administrative task. The proposed closed-loop process enables continuous monitoring, reassessment, and adjustment of rules according to changes in the threat environment, consistent with the continual-improvement and risk-treatment requirements of established information security management standards [16], [17].

The framework also supports improved incident management. By assigning higher priority to events associated with critical assets and repeated attack behavior, security teams can focus their resources on incidents with greater potential impact. This can reduce unnecessary investigation of low-risk events and improve the efficiency of security operations.

However, the proposed approach also has several limitations. The quality of optimization depends directly on the completeness and accuracy of collected logs, the correctness of SIEM correlation rules, and the appropriateness of risk-weighting coefficients. Poorly configured log sources or inaccurate risk parameters may lead to incorrect prioritization. In addition, automated policy adjustments should be controlled by security specialists because fully automatic rule modification may create unintended service disruptions or security gaps. Comparable cautions have been raised regarding the operational deployment of automated detection in network security, where the cost of errors and the difficulty of interpreting outputs limit full automation [18].

Thus, the practical value of the proposed method lies in combining automated analytics with expert validation. SIEM-driven risk assessment can support decision-making, but final WAF policy changes should remain subject to controlled review, testing, and continuous monitoring. This hybrid approach provides a more reliable basis for maintaining effective and adaptive web application protection in modern data center infrastructures.

## Conclusion

The study demonstrates that risk-based optimization of Web Application Firewall policies can be strengthened through the integration of SIEM-driven log analytics. The proposed framework combines WAF event monitoring, centralized log correlation, contextual risk scoring, rule evaluation, and iterative policy adjustment within a continuous security management cycle.

The analysis shows that WAF policies should not be evaluated only by the number of triggered alerts. A more effective approach requires consideration of attack severity, asset criticality, event recurrence, detection confidence, vulnerability exposure, and correlated security evidence. This makes it possible to distinguish high-risk threats from low-impact anomalies and to identify rules that generate excessive false positives or no longer correspond to the current application environment.

The proposed methodology also supports more efficient incident prioritization. By correlating WAF events with authentication logs, application activity, network telemetry, and other SIEM data, security analysts can obtain a broader understanding of attack behavior and focus resources on incidents with greater potential impact.

An important advantage of the framework is its adaptive character. The optimization process is organized as a closed loop in which WAF rules are periodically reassessed and adjusted according to newly observed attack patterns, system changes, and vulnerability information. This approach is more appropriate for dynamic data center environments than static rule configuration.

At the same time, the effectiveness of the framework depends on the quality of log collection, correlation logic, risk-weighting parameters, and expert validation. Therefore, automated analytics should support, rather than completely replace, security specialists in WAF policy management.

In conclusion, SIEM-driven risk analysis provides a practical methodological basis for improving WAF policy accuracy, reducing unnecessary alerts, strengthening incident prioritization, and

increasing the adaptability of web application protection in data center environments. Future research should focus on experimental validation of the proposed framework using real operational logs and measurable indicators such as false-positive rate, detection accuracy, incident triage time, and rule optimization efficiency.

## REFERENCES


[1] OWASP Foundation, "OWASP Top 10: The ten most critical web application security risks," OWASP, 2021. [Online]. Available: https://owasp.org/Top10/

[2] OWASP Foundation, "OWASP ModSecurity Core Rule Set (CRS)," OWASP. [Online]. Available: https://coreruleset.org/

[3] OWASP Foundation, "ModSecurity frequently asked questions (FAQ): Configuration and detection-only mode," OWASP ModSecurity Project. [Online]. Available: https://github.com/owasp-modsecurity/ModSecurity/wiki/

[4] ModSecurity.io, "Rule exclusions and safe tuning: Guidance on false-positive reduction and narrow WAF rule exclusions." [Online]. Available: https://modsecurity.io/

[5] S. Axelsson, "The base-rate fallacy and the difficulty of intrusion detection," ACM Transactions on Information and System Security, vol. 3, no. 3, pp. 186–205, 2000, doi: 10.1145/357830.357849.

[6] K. Kent and M. Souppaya, "Guide to computer security log management," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-92, 2006, doi: 10.6028/NIST.SP.800-92.

[7] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security Operations Center: A systematic study and open challenges," IEEE Access, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

[8] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-30 Rev. 1, 2012, doi: 10.6028/NIST.SP.800-30r1.

[9] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST CSWP 29, 2024, doi: 10.6028/NIST.CSWP.29.

[10] Joint Task Force, "Risk management framework for information systems and organizations: A system life cycle approach for security and privacy," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-37 Rev. 2, 2018, doi: 10.6028/NIST.SP.800-37r2.

[11] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-94, 2007, doi: 10.6028/NIST.SP.800-94.

[12] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System version 3.1: Specification document," FIRST, 2019. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[13] C. Kruegel and G. Vigna, "Anomaly detection of web-based attacks," in Proc. 10th ACM Conf. Computer and Communications Security (CCS '03), Washington, DC, USA, 2003, pp. 251–261, doi: 10.1145/948109.948144.

[14] MITRE Corporation, "MITRE ATT&CK: Adversarial tactics, techniques, and common knowledge," MITRE. [Online]. Available: https://attack.mitre.org/

[15] National Institute of Standards and Technology, "NIST Cybersecurity Framework 2.0: Enterprise risk management quick-start guide," Gaithersburg, MD, USA, NIST Special Publication 1303, 2024.

[16] Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements, ISO/IEC Standard 27001:2022, Geneva, Switzerland, 2022.

[17] Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks, ISO/IEC Standard 27005:2022, Geneva, Switzerland, 2022.

[18] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in Proc. IEEE Symp. Security and Privacy, Oakland, CA, USA, 2010, pp. 305–316, doi: 10.1109/SP.2010.25.