Application Security Analyzer Using SIEM Tool

Udutha shashidhar

Department of Cyber Security

shashi400066@gmail.com

# Abstract - The "Application Security Analyzer Using SIEM Tool" (ASA) project represents a pivotal advancement in bolstering organizational security measures. ASA serves as a sophisticated tool tailored to scrutinize system events within an organization's infrastructure. Leveraging the capabilities of a Security Information and Event Management (SIEM) tool, ASA enables the centralized monitoring and analysis of system events, providing administrators with invaluable insights into potential security threats and vulnerabilities. Moreover, ASA's integration with cloud technology further enhances its utility by facilitating remote management and control of organizational systems. This cloud connectivity empowers administrators to swiftly deploy patches, updates, and enact system controls from any location, thereby ensuring the continuous protection of critical assets. In essence, the implementation of ASA offers organizations a comprehensive solution to proactively identify and address security risks, ultimately safeguarding their digital infrastructure and ensuring business continuity in an increasingly interconnected world.

**Keywords –** Application Security Analyzer, SIEM, cloud technology, organizational security, centralized monitoring, threat detection, remote management capabilities.

# Introduction

"Application Security Analyzer" (ASA) project: ASA serves as a vital tool for scrutinizing system events within organizational infrastructures, leveraging the centralized recording and analysis capabilities provided by a Security Information and Event Management (SIEM) tool. Through this centralized approach, ASA enables comprehensive event analysis to identify potential security threats and vulnerabilities effectively. Furthermore, ASA's integration with a cloud platform facilitates remote access and management, empowering administrators to deploy patches, updates, and system controls seamlessly to bolster organizational security measures. Overall, the ASA project represents a significant advancement in enhancing cybersecurity protocols and safeguarding organizational assets against evolving threats. ASA

empowers organizations to meticulously scrutinize system events within their infrastructure. This centralized approach facilitates comprehensive event analysis, enabling the proactive identification and mitigation of potential security threats and vulnerabilities. Moreover, ASA's seamless integration with a cloud platform empowers administrators with remote access and management capabilities. This allows for the swift and efficient deployment of patches, updates, and system controls, further fortifying the organization's security measures. In Overall, the ASA project complex activity which must understandthe content and capture the hidden sentiments in the written text from which itis inevitable to study new methods.

At its core, ASA serves as a comprehensive solution built upon the foundation of a Security Information and Event Management (SIEM) tool. This foundation provides a centralized platform for collecting, storing, and analyzing security-related events from various sources across an organization's network, including applications, operating systems, network devices, and user activity. By leveraging this centralized approach, ASA empowers security personnel with the ability to conduct in-depth analysis of these events, enabling them to identify and understand potential security threats and vulnerabilities in a timely and efficient manner.

However, the functionality of ASA extends beyond simple log collection and analysis. By integrating with vulnerability scanners and threat intelligence feeds, ASA becomes a proactive threat detection engine. Vulnerability scanners identify weaknesses within applications and operating systems, allowing for swift remediation and reducing the attack surface. Meanwhile, threat intelligence feeds keep ASA up-to-date on the latest attack vectors and emerging threats, enabling organizations to adjust their security postures proactively to stay ahead of evolving threats.

Furthermore, ASA goes beyond mere threat detection by facilitating efficient response and remediation. Its centralized log management and analysis capabilities provide security teams with a consolidated view of security incidents, allowing for faster and more comprehensive investigation workflows.

This streamlined approach reduces the time spent identifying the root cause of an incident and enables organizations to take swift and decisive action to mitigate the threat and minimize damage.

Beyond proactive threat detection and incident response, ASA offers significant benefits in terms of compliance and cost reduction. By generating detailed reports demonstrating compliance with relevant security regulations and standards, ASA simplifies compliance audits and provides organizations with verifiable documentation of their commitment to data security. Additionally, by automating tasks such as log analysis and vulnerability scanning, ASA streamlines security operations, freeing up valuable time and resources for security personnel to focus on strategic initiatives.

# Techniques for Application Security Analyzer (ASA) using Security

* 1. **Log Collection and Normalization:**

**Centralized SIEM logging:** Leverage SIEM capabilities to collect security logs from various sources, including applications, operating systems, network devices, and user activity.

**Log normalization:** Normalize collected logs into a common format for easier parsing, analysis, and correlation across different data sources.

# Anomaly Detection and Event Correlation:

**Develop advanced correlation rules:** Define rules that identify suspicious patterns and relationships between security events to detect potential threats and vulnerabilities.

**Utilize threat intelligence feeds:** Integrate threat intelligence feeds into ASA to stay informed about the latest attack vectors and threat indicators, allowing for proactive threat detection.

**Machine learning and anomaly detection:** Explore the use of machine learning algorithms to identify anomalous events that deviate from established baselines, potentially revealing security incidents.

# Vulnerability Assessment and Prioritization:

**2.5 Additional Techniques:**

**User and entity behavior analytics (UEBA):** Analyze user and entity behavior patterns to identify suspicious activities that could indicate potential insider threats or compromised accounts.

**Deception technology:** Deploy deception technology within the network to lure attackers into interacting with fake assets, revealing their presence and intentions.

**Continuous security monitoring:** Implement continuous security monitoring practices to maintain a constant vigil on security events and identify threats in real-time.

# Existing System

The existing system relies on a central SIEM tool to analyze security events, offering a unified perspective for detecting threats. Yet, its vulnerability stems from the absence of remote management features, slowing down incident response and limiting administrative oversight of dispersed systems across different locations.

The ASA project emerges as a solution to bridge this gap. By integrating with a cloud platform, ASA empowers administrators with remote access to security controls, allowing for swifter deployment of patches and improved response to security incidents. Additionally, ASA has the potential to leverage advanced threat detection methods, potentially including vulnerability scanners and threat intelligence feeds, offering a more comprehensive security posture against evolving threats. In essence, ASA represents a significant leap forward, transforming security from a reactive to a proactive approach.

Relies on a centralized SIEM tool for analyzing system events within the organization. However, it lacks direct connectivity to a cloud platform for remote management and control of organizational systems.

* Systematic Review of Web Application Security Vulnerabilities Detection Methods (2015)

# Strengths:

**Integrate vulnerability scanners:** Integrate vulnerability scanning tools with ASA to identify weaknesses within applications and operating systems.

**Prioritize vulnerabilities:** Analyze vulnerabilities based on severity, exploitability, and potential impact to prioritize remediation effort.

# 2.4 Incident Response and Remediation:

**Incident timeline and investigation:** Utilize centralized log data to establish a comprehensive timeline of security incidents, facilitating investigation workflows.

**Automated remediation:** Implement automated remediation actions based on pre-defined rules, such as patching vulnerabilities or isolating compromised systems.

**Centralized Security Monitoring:** The SIEM tool offers a consolidated view of security events across the organization, enabling efficient analysis and threat detection.

# Weaknesses:

**Limited Remote Management:** Inability to directly connect to a cloud platform restricts remote access and control of systems.

**Incident Response:** Delays in deploying patches, updates, or isolating compromised systems during security incidents.

**Administrative Efficiency:** Inconvenience in managing security from remote locations.

**Scalability:** Difficulty in managing geographically distributed systems.

# Potential Security Gaps:

**Reliance on Outdated Methods:** The lack of information about advanced threat detection capabilities suggests the system might rely on older techniques, potentially leaving vulnerabilities undetected.

How ASA Project Addresses These Issues:

The ASA project aims to bridge the gap by introducing the following functionalities:

**Cloud Platform Integration:** Enables secure remote access and management of security controls from anywhere.

**Enhanced Threat Detection:** Potential integration with vulnerability scanners and threat intelligence feeds can provide a more comprehensive view of the threat landscape and identify sophisticated attacks.

**Improved Response Times:** Faster deployment of patches and security measures due to remote management capabilities.

# Limitations of the Existing System:

The current system suffers from several shortcomings that hinder its effectiveness in safeguarding organizational security:

**Lack of Remote Management:** Inability to access and control systems remotely restricts response times to security incidents and hampers administrative efficiency, especially for geographically dispersed organizations.

**Dependency on Manual Intervention:** Manual processes for security tasks can be slow, error-prone, and labor-intensive, leaving the system vulnerable during gaps in monitoring.

**Inefficient Response to Security Threats:** Delayed response due to manual intervention and limited remote access can exacerbate the impact of security incidents, potentially leading to data breaches and disruptions.

**Potential Disruption to Business Operations:** Security incidents and the time required for manual remediation can disrupt core business functions, leading to productivity loss and financial repercussions.

**Limited Scalability and Adaptability:** The system might struggle to adapt to evolving security threats and accommodate growth within the organization, requiring significant manual effort for adjustments.

# Proposed System

The proposed system offers several significant advantages over the existing one, addressing the limitations mentioned previously.

# Enhanced Remote Management Capabilities:

**Streamlined Security Operations:** Administrators can remotely access and manage security controls from anywhere, enabling faster decision-making and improved response times.

**Centralized Patch Deployment:** Patches and updates can be deployed across the organization remotely, ensuring consistent security posture and reducing the risk of vulnerabilities.

**Improved Administrative Efficiency:** Remote management eliminates the need for physical presence at individual systems, saving time and resources.

# Improved Response Time to Security Threats:

**Faster Detection and Isolation:** The system can automatically detect and isolate threats, minimizing the potential damage and impact on business operations.

**Automated Remediation Actions:** Pre-defined actions can be triggered to automatically contain threats, such as quarantining infected systems or blocking malicious traffic.

**Real-time Threat Monitoring:** Continuous monitoring allows for immediate identification and response to security incidents.

# Seamless Integration with Organizational Infrastructure:

**Centralized Security Management:** The system integrates seamlessly with existing security tools and infrastructure, providing a unified platform for security operations.

**Reduced Complexity:** Streamlines security processes and eliminates the need for managing multiple disparate tools.

**Improved Visibility:** Provides a comprehensive view of the security landscape across the organization.

# Scalability and Adaptability:

**Automatic Scaling:** The system can automatically scale to accommodate growth within the organization or changing security needs.

**Adaptable to Evolving Threats:** The system can be easily updated with new threat intelligence and security measures to address emerging challenges.

**Reduced Manual Intervention:** Automates routine tasks, freeing up IT staff to focus on strategic security initiatives.

# Analysis of Log Data:

**Log Aggregation and Normalization:** IBM QRadar collects log data from various sources such as network devices, servers, applications, and endpoints. Upon ingestion, QRadar normalizes the log data to a standardized format, ensuring consistency and compatibility for analysis. Through normalization, QRadar categorizes log events based on predefined parsers and extracts relevant information such as source IP addresses, timestamps, event types, and severity levels. This process enables uniformity in log data representation, simplifying subsequent analysis tasks.

**Correlation and Threat Detection:** Once log data is normalized, IBM QRadar applies correlation rules and algorithms to detect patterns and anomalies indicative of potential security threats. By correlating events across multiple data sources, QRadar can

uncover complex attack scenarios that may span different layers of the IT infrastructure. QRadar's correlation engine identifies relationships between seemingly unrelated events, facilitating the detection of suspicious behaviors and attack vectors. Additionally, QRadar leverages threat intelligence feeds and behavioral analytics to enrich its analysis, enhancing the accuracy of threat detection and reducing false positives.

# SIEM Architecture

* 1. **Data Collection:**

**Event Collector:** This collects events from various log sources such as firewalls, routers, windows and Unix servers. These events can include security events, system events, and application events.

**Flow Collector:** This collects flow data from network devices such as routers and switches. Flow data includes information about the source and destination of network traffic, as well as the type of traffic and the amount of data transferred.

**Log Source:** This represents any device or application that generates logs that can be collected by QRadar. Examples include syslog servers, proxy servers, and Windows servers.

# Data Processing:

**Event Processor:** This processes event data by parsing the data, extracting relevant fields, and enriching the data with additional information from external sources.

**Flow Processor:** This processes flow data by aggregating the data and identifying trends.

**Parsing:** This involves breaking down log data into its constituent parts, such as timestamps, source IP addresses, destination IP addresses, and event messages.

**Normalization:** This involves converting log data into a common format so that it can be processed and analyzed more easily.

# Data Searches and Analysis of Logs:

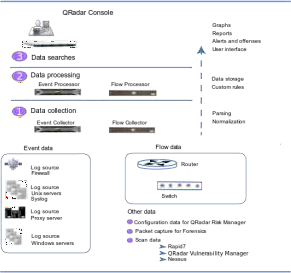
**User Interface:** This provides users with a way to search QRadar data and analyze logs. Users can search for events based on a variety of criteria, such as source IP address, destination IP address, event type, and event message.

**Custom Rules:** These allow users to create custom searches and filters to identify specific security events.

**Reports and Offenses:** These are used to present the results of data searches in a user-friendly format. Reports can be used to identify trends and patterns in security events, while offenses can be used to track and investigate potential security incidents.

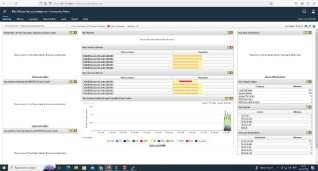
**Graphs:** These can be used to visualize data and identify trends. For example, a graph could be used to show the number of security events over time, or the number of security events by source IP address.

**Data Storage:** This stores the collected and processed data for later analysis.

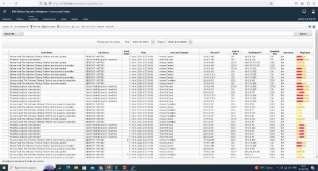


**Figure 1: Architecture of IBM Qradar SIEM**

1. **Results**



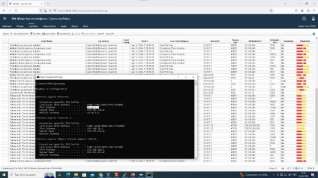
**Figure 2: IBM Qradar Dashboard**



**Figure 3: Collecting Logs from Host**



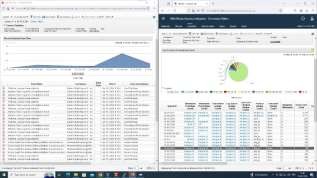
**Figure 4: Rule Making (Potential local port scan)**



**Figure 5: Rule Testing (Potential local port scan)**



**Figure 6: Log Activity Pie chart based on events**



**Figure 7: Events of a particular IP address**

1. **Datasets for Application Security Analyzer (ASA) using SIEM Tool**
   1. **Security Event Logs:**

**System Logs:** Operating system logs containing information about system events, errors, and security-related activities.

**Application Logs:** Logs generated by web applications, including user activity, access attempts, errors, and security events.

**Network Logs:** Network device logs capturing network traffic information, potential intrusions, and suspicious activity.

**Firewall Logs:** Logs recording firewall activity, including blocked traffic, allowed connections, and attempted breaches.

# Vulnerability Scanner Data:

Reports from vulnerability scanners identifying weaknesses and potential security holes within applications and systems.

# Threat Intelligence Feeds:

Real-time or aggregated data feeds containing information about known threats, vulnerabilities, Indicators of Compromise (IOCs), and attacker tactics, techniques, and procedures (TTPs).

# User Activity Data:

User login attempts, access requests, file operations, and other activities that can be analyzed for anomalous behavior.

# Conclusion

Security Information and Event Management (SIEM), a methodology, facilitates threat identification, incident handling, and security incident management by collecting and scrutinizing security events. It empowers organizations to swiftly aggregate and arrange log data from all digital assets in a centralized repository. This section delves into an examination of several Windows events, while similarly, flow data can also undergo analysis.

SIEM not only aids in the consolidation of log data but also offers advanced analytics capabilities to detect and respond to security threats effectively. By leveraging SIEM, organizations can gain insights into their network activities, enabling proactive security measures and enhancing overall cybersecurity posture.

# References

[1]. MukeshYadav, Dhirendra S Mishra, “Study of challenges faced by Enterprises using Security Information and Event Management (SIEM)” Journal of University of Shanghai for Science and Technology, 2021, Vol 23(08), pp. 511-522

[2].SajadHomayoun, AliDehghantanha, MarziehAhmadzadeh, SattarHashemi, RaoufKhayami, “Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence” IEEE Transactions on Emerging Topics in Computing2020, pp. 341-351, vol. 8.

[3]. Giorgi Sharia, “Comparative Analysis of Enterprise Security Information and Event Management (Siem) Solutions, Case Of Cybers” Thesis report, InfotehnoloogiaTeaduskond, 2020.

[4].A.D.Moskvichev, M.V. Dolgachev, "System of Collection and Analysis Event Log from Sources under Control of Windows

Operating System" International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon),2020.

[5]. On SivaramanEswaran, Aruna Srinivasan, Prasad Honnavalli, "A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise"PES University, Bangalore,3 Nov 2021.