From Reactive to Proactive: Automating IP Threat Intelligence in SIEM Systems for Cyber Threat Detection

Original Scientific Paper

Abeer Alhuzali *
King Abdulaziz University,
Faculty of Computing and Information Technology, Department of Computer Science
Jeddah, Saudi Arabia
aalhathle@kau.edu.sa

Asrar Alshareef
King Abdulaziz University,
Faculty of Computing and Information Technology, Department of Computer Science
Jeddah, Saudi Arabia
aalshareef0190@stu.kau.edu.sa

*Corresponding author

Abstract *– Digital transformation has provided more opportunities for cybercriminals and exposed organizations to sophisticated threats. Organizations should continuously evaluate their security measures and implement defensive actions to prevent attacks by cybercriminals. Security Information and Event Management (SIEM) systems, deployed within Security Operations Centers (SOCs), allow organizations to identify security risks and vulnerabilities, monitor unusual behavior, and automatically respond to security events. However, SIEM platforms require certain functional enhancements. For instance, security analysts often use external threat intelligence platforms to check suspicious IP addresses manually. This results in longer response times and a greater likelihood of human error. Hence, this paper proposes an integration framework that correlates the functionality of an external threat intelligence platform (AbuseIPDB) with a SIEM system (IBM QRadar) to automatically validate suspicious IP addresses without the need for manual checking. The goal of this integration is to increase the efficiency of threat analysis, incident response, and SIEM-based threat detection. Tests demonstrated that our proposed framework shortens the threat validation time by up to 97.7%, compared to manual processes. Additionally, our system reduces false positives by capitalizing on contextual threat intelligence, thus allowing SOC teams to prioritize critical alerts.*

Keywords: *SIEM, Security Operations Center (SOC), threat intelligence, IP threat, integration*

Received: July 26, 2025; Received in revised form: September 27, 2025; Accepted: September 29, 2025

1. INTRODUCTION

The extensive adoption of technology increases security vulnerabilities because cyberattacks proliferate and organizational IT systems become vulnerable to sophisticated threats. Kuzio *et al.* [1] identified a marked rise in cyberattacks between 2016 and 2023, including ransomware, cyber fraud, and attacks on critical infrastructure. Countries lacking adequate cybersecurity measures were particularly vulnerable. Thus, organizations require advanced security solutions capable of large-scale data analysis and proactive threat detection to prevent data breaches and protect vital assets [2].

Security Information and Event Management (SIEM) systems have emerged as core technologies within Security Operations Centers (SOCs). SIEM platforms are deployed to collect, correlate, and analyze log data from diverse sources. Nonetheless, SIEM platforms face critical limitations, particularly their inability to validate

suspicious IP addresses autonomously. Hence, security analysts have to investigate such indicators manually using external threat intelligence platforms [3]. This reliance on manual processes results in delays and increases the risk of human error.

Several studies [4–7] have sought to solve this problem by introducing automated integration frameworks for SIEM systems and threat intelligence platforms. However, those studies faced several limitations. For example, they overlooked the impact of real-time integration on the performance of SIEM tools. Additionally, only a few studies have addressed the integration of SIEM systems and IP threat intelligence platforms, which are crucial for enhancing the accuracy of the former.

Therefore, this paper addresses the abovementioned limitations by integrating a reliable external threat intelligence platform (AbuseIPDB) with a SIEM system (IBM QRadar). This study demonstrates how such an integration can automate the validation of suspicious IP addresses, improving detection accuracy, alleviating the burden on analysts, and expediting incident response within enterprise environments. Our work makes the following contributions:

- It develops a systematic and modular integration framework combining IBM QRadar and a threat intelligence platform.
- It shows how to automate IP-related threat analysis in QRadar to reduce reliance on manual tools and shorten incident response time.
- It enhances threat detection accuracy using AbuseIPDB to classify malicious IP addresses based on global data.
- It enables the automated generation of reports to improve the speed and precision of decision-making for security analysts.
- It comprehensively evaluates the integration framework to assess its effect on the SIEM.

The remainder of this paper is organized as follows: Section 2 provides background information and Section 3 reviews related work. Section 4 describes the methodology used for the integration. Section 5 details the implementation process and system configuration. Section 6 analyzes the results. Finally, Section 7 concludes the paper and provides recommendations for future research.

2. BACKGROUND

2.1. COMPUTER SECURITY INCIDENT RESPONSE TEAMS

Computer Security Incident Response Teams (CSIRTs) receive, analyze, and respond to security issues affecting data and computer systems. CSIRTs work within organizations, governments, or regions [8]. These teams monitor security events to detect unusual activity that may endanger the information technology (IT) assets of their organizations. They provide reactive services (e.g., incident analysis and response coordination) and proactive services (e.g., vulnerability handling, threat analysis, and cybersecurity information dissemination). They also raise awareness and act as central contact points for incident reporting. Their success relies on four fundamental principles: technical excellence to ensure adequate guidance and solutions, trust to encourage sharing sensitive information, resource efficiency for effective responses, and cooperation with internal and external stakeholders [9]. CSIRTs generally work within SOCs, which are centralized units belonging to IT departments. SOCs continuously monitor, analyze, and respond to security events to detect threats [10].

2.2. SECURITY INFORMATION AND EVENT MANAGEMENT

SIEM systems collect and analyze logs from various sources, including firewalls, intrusion detection and prevention systems (IDS/IPS), and servers [11]. SIEM platforms integrate advanced tools, such as User and Entity Behavior Analytics (UEBA) and machine learning, to improve threat detection and support data-driven decision-making. Using these systems, administrators can define security policies and manage events from multiple sources.

SIEM architecture includes elements for log collection, normalization, analysis, rule-based correlation, storage, and continuous monitoring. Each module can function independently; however, their integration is crucial for optimal system performance [12]. Fig. 1 shows a simplified view of the SIEM log-processing workflow, illustrating how data is normalized and analyzed for monitoring and incident response [10].

Fig. 1. Simplified SIEM log processing workflow: from log collection to monitoring (source: [10]).

2.3. IBM QRADAR

IBM developed QRadar, one of the top SIEM systems, designed to help organizations monitor threats and manage security incidents. QRadar employs machine learning and user behavior analytics to detect unusual activities and enable fast responses [13]. This system gathers and analyzes event data and network flows from various sources, including operating systems, endpoints, and applications. Then, it correlates this information to generate unified alerts that facilitate security investigations. QRadar is a commercial product and thus employs proprietary software and a licensing system that grants IBM full control over the source code. QRadar enhances security and helps organizations fight cyber threats.

Fig. 2 illustrates QRadar's system architecture, highlighting its components for data collection, processing, and analysis [14]. QRadar's first layer collects and normalizes log events and network flows from various sources, converting them into structured data for analysis. The Custom Rule Engine (CRE) layer analyzes event and flow data in real-time; it evaluates rules and building blocks to trigger alerts when security conditions are met. Security analysts use QRadar's GUI to search, filter, and investigate processed data for reporting and offense analysis.

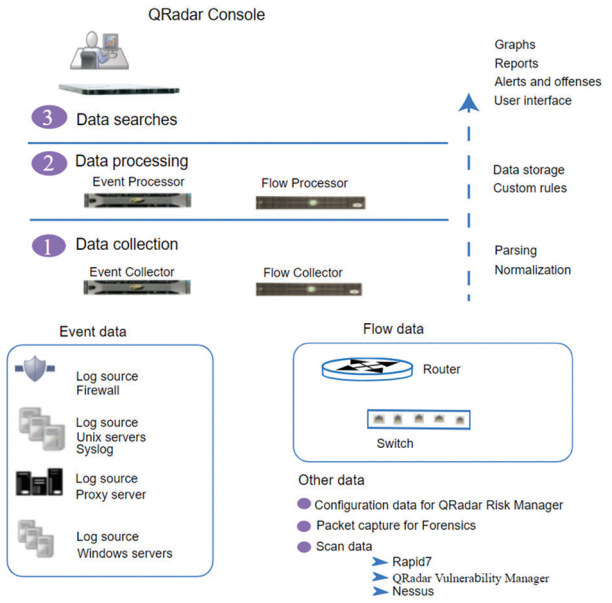

Fig. 2. IBM QRadar system architecture: data collection, processing, and analysis (source: [14]).

2.4. IP THREAT INTELLIGENCE

IP threat intelligence is the use of timely and reliable information on IP addresses associated with malicious activities, such as cyberattacks, system intrusions, or botnet command and control. Thus, IP threat intelligence is key for enhancing the capability of security systems to detect and respond to threats, particularly when integrated with log analysis platforms, such as SIEM systems [15].

2.5. IP-BASED THREAT INTELLIGENCE FEEDS

Threat intelligence feeds are used for collecting Indicators of Compromise (IoCs), including malicious IP addresses. Acquiring accurate and up-to-date information about adversarial behavior enables defenders to refine their security practices and reduce the window of vulnerability, defined as the period during which an organization remains exposed because of a lack of awareness of current attack techniques. Organizations increasingly rely on third-party providers to collect, filter, and curate threat intelligence data, given the complexity of developing such intelligence. The growing market demand in this domain has contributed to notable investments and operational interest [16].

2.6. ABUSEIPDB

AbuseIPDB provides an API that enables users to retrieve detailed information about an IP address, including whether it is blacklisted, its associated geolocation, and the types of threats attached to it. AbuseIPDB is more effective in detecting malicious IP addresses than other public databases; thus, it is recognized as one of the most reliable tools for IP reputation analysis. Lewis *et al.* [17] conducted a comparative evaluation and reported that AbuseIPDB detected 46% of malicious IP addresses, outperforming VirusTotal (13%) and MyIP.ms (16%).

Furthermore, researchers have used AbuseIPDB to investigate IP addresses associated with Advanced Persistent Threat (APT) campaigns, such as *Grizzly Steppe* and *Hidden Cobra*. AbuseIPDB facilitates the collection of rich metadata, such as country codes, activity patterns, and behavioral indicators, and thus enables the precise profiling of malicious infrastructure [18].

These results demonstrate AbuseIPDB's reliability and near real-time capability for assessing IP reputation. The accuracy and accessibility of AbuseIPDB make it a popular choice in academia and enterprise security operations. Fig. 3 shows AbuseIPDB's web interface, which supports IP reporting, historical IP searches, and access to reputation data through the public API.

Fig. 3. AbuseIPDB web interface for IP reputation checking (source: [19])

3. RELATED WORK

Recent studies have emphasized the advantage of integrating SIEM platforms with external threat intelligence sources to improve detection accuracy and reduce false positives [4, 5, 7].

For example, Owen [4] reported that incorporating threat intelligence feeds into SIEM systems augments alert precision and provides security analysts with rich insights through visual dashboards. Owen showed that such a synergistic system enhanced SIEM's capabilities by providing up-to-date information on malicious actors, boosting performance, and addressing data gaps. Similarly, Smeriga [5] explored ways for integrating Cisco Global Threat Alerts [20] with third-party SIEM solutions, emphasizing the need for flexible integra-

tion through efficient APIs. Smeriga also introduced interactive dashboards to help analysts with data interpretation and analysis. Suskalo *et al.* [13] compared IBM QRadar and Wazuh [21], two popular SIEM tools. They found that QRadar exhibits integration flexibility, but requires careful tuning for open-source intelligence feeds, such as AbuseIPDB. By contrast, Wazuh showed robust threat detection and log analysis capabilities, supported by an active user community. The authors presented practical scenarios illustrating how both platforms responded to different attack attempts and evaluated the accuracy of their alerts. Their findings were useful for our selection of IBM QRadar as the SIEM for the current work. Tulcidas [6] proposed using Snort [22], an open-source IDS, and integrating it with Wazuh, an open-source SIEM, in a large-scale academic network. The integration reduced false alarms by enriching events and correlating them with external sources, enabling a faster and more accurate response to internal and external attacks. Tulcidas also compared various SIEM solutions, highlighting their differences in core functionalities, such as aggregation, analysis, and compliance. Sauerwein and Staiger [23] evaluated 13 threat intelligence-sharing platforms, including MISP, OpenCTI, and OTX, using over 50 functional and non-functional criteria that covered aspects including data collection, processing, analysis, dissemination, and integration. However, they noted gaps in data reliability and quality. Although they excluded AbuseIPDB from their analysis, their study provided valuable insights into the factors to consider when selecting a platform. Esseghir *et al.* [7] proposed an open-source platform combining SIEM and IDS functionalities for network monitoring and security alert management. Their proposed system can detect malware in encrypted network traffic using heuristics within a decision tree model. Other studies have investigated the use of machine-learning algorithms to detect cyber-attacks, such as DDoS [24] and other network traffic intrusions [25].

Integrating IBM QRadar with external threat intelligence feeds like AbuseIPDB shows potential for enhancing security monitoring. However, there are no structured methods for combining QRadar with AbuseIPDB. Thus, we propose a novel integration that automates IP reputation analysis to improve response times and accuracy.

4. INTEGRATION METHODOLOGY

Here, the AbuseIPDB reputation platform is integrated with IBM QRadar to automate the analysis of suspicious IP addresses. The proposed system improves threat detection precision and the response to cyber incidents.

4.1. PLATFORM SELECTION RATIONALE

IBM QRadar can collect, analyze, and correlate event logs; thus, it was chosen as the integration platform. Furthermore, QRadar supports the creation of custom correlation rules to generate security alerts. Its flexibility, scalability, and support for threat intelligence make it a popular choice in the cybersecurity industry. AbuseIPDB was selected as the external threat intelligence source because of its extensive database of malicious or suspicious IP addresses and its API, which allows direct reputation searches.

Combining these tools results in an automated workflow that extracts IP addresses from incoming logs, checks their reputation through AbuseIPDB, and returns the enriched data to QRadar. This setup allows QRadar to take suitable security actions based on the classification results.

4.2. SYSTEM ARCHITECTURE

We propose a framework that integrates a malicious IP address reputation service (AbuseIPDB) with a SIEM platform (IBM QRadar). Fig. 4 depicts the framework and its components.

The Integration Control and Management (ICM) module, which oversees the integration process, is at the heart of the system. The ICM handles communication with AbuseIPDB and QRadar. As a result, a final security report is generated for each analyzed IP address. To initiate an analysis, the ICM sends a Syslog message containing the IP address in the Check-IP= xxx.xxx.xxx.xxx format. These messages follow the RFC-5424 standard to ensure QRadar can parse them correctly. The messages are transmitted via the UDP protocol to a predefined port (for example, 5514) on the server running the ICM listening service.

The ICM operates as a background service that continuously monitors the assigned port. When a new message arrives, the ICM uses a regular expression to extract the IP address from the content. The obtained IP is then submitted to AbuseIPDB for a reputation check. AbuseIPDB provides details, such as a confidence score, the country code associated with the IP address, and the date of the most recent reported incident. The confidence score, ranging from 0 to 100, reflects the likelihood that the IP address is linked to malicious activity, based on the number of incident reports.

Then, the ICM uses this data to evaluate the risk level of the IP, which is classified according to its confidence score:

- High-risk: score ≥ 75
- Medium-risk: $20 \leq$ score < 75
- Low-risk: score < 20

This classification is associated with the color-coded ranges in the AbuseIPDB interface. Red indicates high risk, orange denotes medium risk, and yellow represents low risk. This method was validated by testing on real IP data. As a result, IPs with higher confidence scores were consistently associated with multiple abuse reports and malicious behavior. Therefore, we adopted this three-tier classification to enhance the QRadar analysis [19].

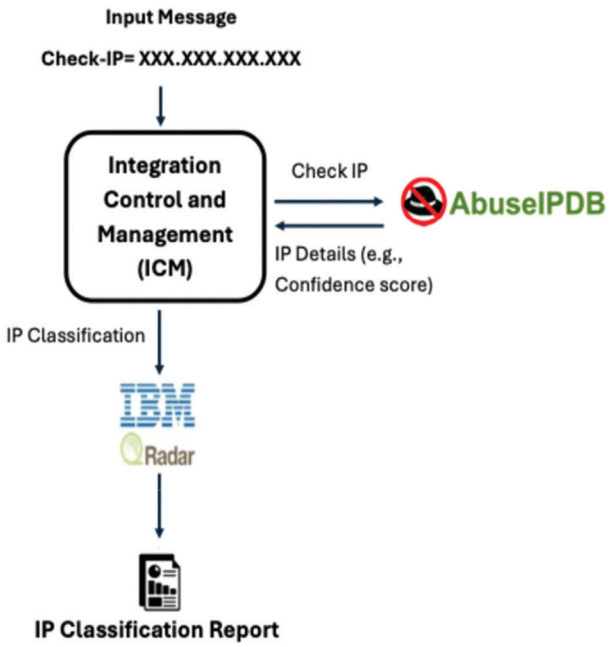

Fig. 4. System architecture for QRadar-AbuseIPDB integration (source: created by the authors)

After the classification process is completed, the ICM re-formats the results into a Syslog-compliant message that includes key data, such as the IP address, country, confidence score, category, and the last reported date. This message is then transmitted to the QRadar platform via UDP, using a custom log source identifier. Next, a custom data source module (DSM) receives and parses the message. If the IP address is classified as high risk or medium risk, the ICM generates a detailed analytical report that lists the IP address, country, confidence score, category, and last reported date, together with analyst-oriented notes tailored to the risk level. The report is automatically stored in a designated network folder, and its file path is inserted into the Syslog message sent to QRadar. This method allows analysts to access the report directly from the event record in *Log Activity*, eliminating the need for manual searching.

5. INTEGRATION IMPLEMENTATION DETAILS

Integration is implemented through the ICM module, which receives request messages, analyzes IP addresses, extracts IP addresses from the messages, assesses their reputation using the AbuseIPDB API, and sends the enriched results back to QRadar through a designated log source. More details are provided in the following sections.

5.1. PHASE ONE: IP MESSAGE CONFIGURATION

The ICM initializes the environment and begins listening for incoming messages. UDP socket port 5514 on the server hosting the ICM's listening service is opened to receive messages from source devices, such as PowerShell scripts running on Windows machines.

5.2. PHASE TWO: PROCESSING SYSLOG MESSAGES AND REPUTATION ASSESSMENT VIA ABUSEIPDB

In this phase, the ICM—a Python code that uses the *socket* library—listens for incoming messages on port 5514. Then, the ICM scans each received message using a regular expression to detect the presence of an IP address; it does this by checking whether the message contains the tag *CHECK-IP*. If the tag is absent, the message is disregarded. Otherwise, the script extracts the IP address. Upon identifying an IP address, the script sends a query to the AbuseIPDB API via an HTTP GET request, using the *requests* library. This request includes a predefined and valid API key. The response, returned in JSON format, provides detailed information about the reputation of the IP address, including the confidence score (a numerical value representing the likelihood that the IP address is malicious), country (a two-letter code indicating the geographic location of the IP address; e.g., US), and the last reported date (the most recent date an abuse report was submitted for this IP). The IP address is classified according to the confidence scores detailed in Section 4.2.

5.3. PHASE THREE: FORMATTING THE ANALYZED DATA AND FORWARDING IT TO QRADAR

Once the IP address is classified according to its risk level, the system generates a message containing the IP address, confidence score, country, last reported date, and final classification (high risk, medium risk, or low risk). This message is built per the structure and formatting requirements of the QRadar platform, following RFC 5424 standards. The message is transmitted to port 514 and received by a designated log source within QRadar for analysis. Then, the message is stored and indexed in the *Log Activity* module.

5.4. PHASE FOUR: CONFIGURING QRADAR TO EXTRACT FIELDS FROM INCOMING MESSAGES

QRadar was configured to extract specific fields from incoming messages by creating custom event properties within the DSM editor. The extraction process relied on precise regular expressions to enable the automatic identification of the following values:

- IP address
- Confidence score
- Country
- Classification
- Last reported date
- Report path

These extracted values were made available within the *Log Activity* module, allowing security analysts to review and analyze each log entry thoroughly.

5.5. PHASE FIVE: ACTIVATING A SECURITY RULE IN QRADAR

After classification, the results are immediately forwarded to QRadar in the form of a Syslog-compliant message. The ICM treats each classification level accordingly. For high-risk IPs, the ICM automatically triggers a security offense via a custom rule. This custom security rule is created within the QRadar platform to automatically trigger an alert upon receiving any message with a *high-risk* classification. This rule is designed to detect high-risk threats without requiring manual intervention. Once triggered, the resulting event is recorded in the *Log Activity* module as a high-priority offense. For *medium-risk* and *low-risk* IPs, the events are logged in the *Log Activity* module without triggering alerts.

5.6. PHASE SIX: FINAL REPORT GENERATION

An analytical PDF report is generated only if the IP address is classified as high risk or medium risk. The report includes key information, such as the IP address, country, confidence score, and last reported date. Furthermore, it provides the security analyst with analytical notes and tailored security recommendations based on the evaluated risk level. Once generated, the report is stored in a predefined shared folder on the network, and the full file path is embedded within the Syslog message sent to QRadar. This mechanism enables analysts to access the report from the event log directly, supports informed decision-making, and contributes to the systematic documentation of analyzed cases. Finally, the ICM returns to its listening state, allowing it to receive and process new messages continuously. The diagram in Fig. 5 depicts the workflow and outlines the steps executed.

6. RESULTS

6.1. EXPERIMENTAL SETUP

The integration framework and experiments were conducted on Oracle VirtualBox with a Red Hat (64-bit) OS, an Intel Core i7-1550H processor of 2.6 GHz, and 8 GB of memory. The integration code was written in Python and used several libraries, including the requests library (detailed in Section 5).

6.2. RESULTS SUMMARY

A series of tests was conducted on 30 randomly selected IP addresses across different confidence score levels from AbusIPDB to evaluate the accuracy of the classification mechanism and the overall effectiveness of the automated response. Table 1 summarizes these selected IPs along with their characteristics. Ten IPs were classified as low risk, 12 as medium risk, and eight as high risk. All of the 30 IPs were correctly classified by our QRadar–AbuseIPDB integration framework. The "Validation Time" column lists the total time required to analyze and categorize each IP automatically. Values ranged from 0.487 seconds (IP# 21) to 18.419 seconds (IP# 17). To compare these results with the manual verification process of each IP, we assumed that manual verification for an IP takes between 30 and 60 seconds. This is reasonable because, in the manual scenario, the analyst must manually verify the IP in AbuseIPDB and then insert the result into the SIEM. For all 30 IPs, the manual process would require between 900 seconds (15 minutes) and 1800 seconds (30 minutes). Hence, our integration framework decreased the threat validation time range by 95%–97.7%.

The integration of QRadar and AbuseIPDB performed well in the real-time analysis of suspicious IP addresses, enabling automated risk-based classification and the generation of security reports to support the incident response team.

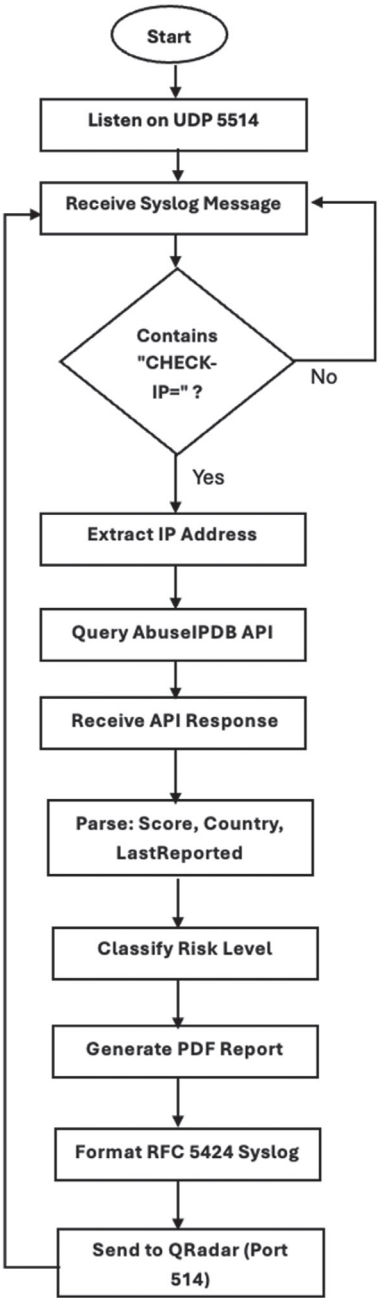

Fig. 5. IP reputation processing workflow (source: created by the authors)

Table 1. IP risk classification results generated by the QRadar–AbuseIPDB integration

#	IP	Score (%)	Country	Classification	Validation Time (sec)
1	209.85.217.42	9	US	Low risk	1.214
2	209.85.167.50	31	FI	Medium risk	0.563
3	216.244.66.245	83	US	High risk	0.690
4	209.85.222.193	64	US	Medium risk	1.615
5	2.57.121.215	54	RO	Medium risk	0.706
6	4.156.21.66	7	US	Low risk	1.145
7	209.85.167.50	31	FI	Medium risk	0.770
8	209.85.222.193	64	US	Medium risk	0.569
9	149.56.160.230	29	CA	Medium risk	0.692
10	209.85.216.66	65	US	Medium risk	0.678
11	185.220.101.26	100	DE	High risk	0.732
12	117.50.47.222	5	CN	Low risk	0.815
13	44.202.169.35	14	US	Low risk	0.568
14	142.4.9.200	18	US	Low risk	0.695
15	185.204.1.182	86	FI	High risk	0.717
16	185.220.101.174	90	DE	High risk	1.268
17	218.92.0.229	100	CN	High risk	18.419
18	77.32.148.7	25	FR	Medium risk	0.637
19	209.85.208.172	26	FI	Medium risk	0.683
20	93.185.162.14	83	ID	High risk	0.601
21	40.107.94.90	2	US	Low risk	0.487
22	103.176.90.16	79	NL	Medium risk	0.723
23	216.239.36.158	1	US	Low risk	0.729
24	209.85.166.230	21	US	Medium risk	0.585
25	88.214.25.62	16	DE	Low risk	1.485
26	146.88.240.123	100	US	High risk	0.593
27	139.59.94.202	15	IN	Low-Risk	0.757
28	216.244.66.236	87	US	High-Risk	0.646
29	209.85.214.200	35	US	Medium-Risk	0.632
30	110.185.37.103	11	CN	Low-Risk	1.065
		Total validation time			**41.479**

6.3. EXAMPLE OF A HIGH-RISK CLASSIFICATION

The IP address *185.204.1.182* was checked by our integration framework, extracted, analyzed, and assigned a high-risk classification (Fig. 6). Therefore, QRadar automatically generated a PDF security report in the specified path (Fig. 7).

The report included the IP address, confidence score, country of origin, last reported date, and tailored mitigation recommendations. All generated reports for high-risk IPs are saved in the "*C:\ThreatReports\High-Risk*" folder, with filenames reflecting the IP address and creation date to facilitate tracking. The full file path of each report was embedded in a Syslog message sent to QRadar via the designated log source. Upon receiving the message, QRadar parsed the content using a custom DSM and extracted the relevant fields. A custom correlation rule within QRadar automatically evaluates the classification field, and if the value is high risk, it triggers an offense of type *Suspicious Activity*.

This offense was logged in the Log Activity module and made visible to analysts, enabling them to access the associated report and take immediate action.

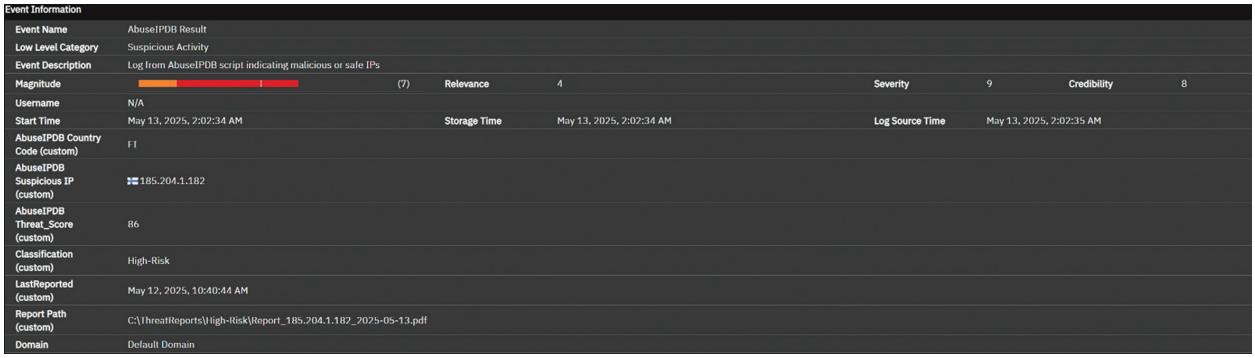

Fig. 6. QRadar's log of high-risk IP 185.204.1.182 (source: created by the authors)

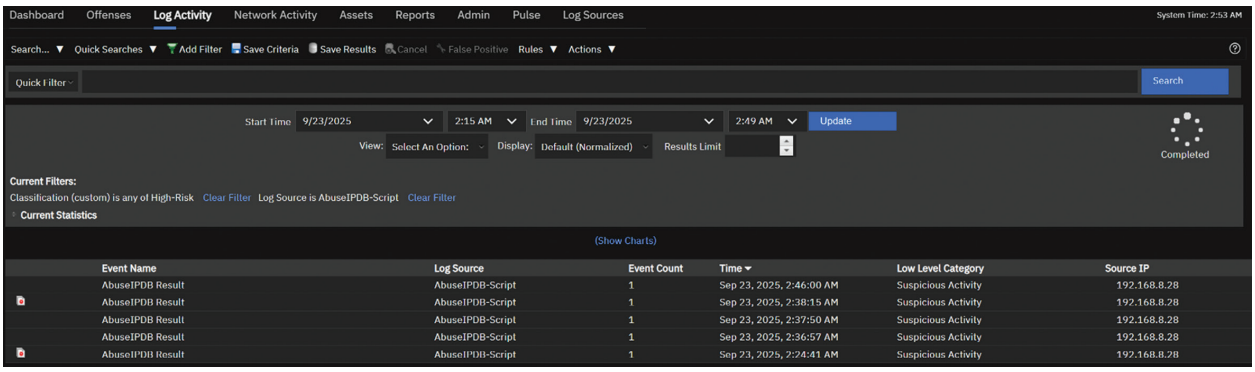

Fig. 7. QRadar's Log Activity module, showing the triggering of a high-risk IP offense (source: created by the authors)

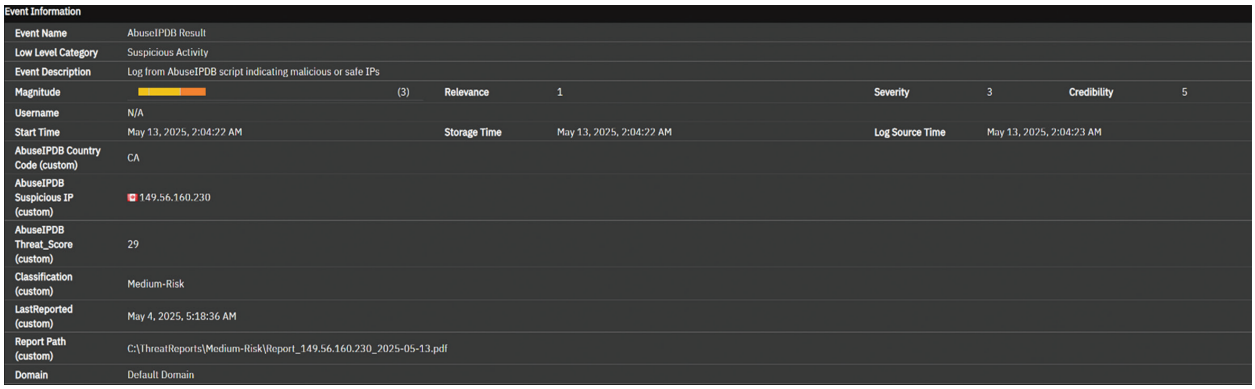

Fig. 8. QRadar's log of medium-risk IP 149.56.160.230 (source: created by the authors)

- **IP address**: *185.204.1.182*
- **Score**: *86%*
- **Country**: *FI*
- **Classification**: *High risk*
- **Last reported**: *May 12, 2025, 10:40:44 AM*
- **Report path**: *C:\ThreatReports\High-Risk\Report_185.204.1.182_2025-05-13.pdf*

6.4. EXAMPLE OF A MEDIUM-RISK CLASSIFICATION

The IP address *149.56.160.230* was classified as medium risk by our tool, based on a confidence score of 29% assigned by AbuseIPDB (Fig. 8). Our system generated a PDF report, which included the IP address, confidence score, country, and the date of the last reported update.

The report was saved in the "*C:\ThreatReports\Medium-Risk*" folder, with a filename including the IP address and creation date. The report also included analytical notes and initial recommendations to help analysts monitor the cases and decide whether escalation is needed if risk levels increase. After the report was generated, our system sent a Syslog message containing the file path and classification result to QRadar. The case was automatically logged in the *Log Activity* module as a medium-severity event without triggering an offense.

- **IP address**: *149.56.160.230*
- **Score**: *29%*
- **Country**: *CA*
- **Classification**: *Medium risk*
- **Last reported**: *May 4, 2025, 5:18:36 AM*
- **Report path**: *C:\ThreatReports\Medium-Risk\Report_149.56.160.230_2025-05-13.pdf*

6.5. EXAMPLE OF A LOW-RISK CLASSIFICATION

IP address *117.50.47.222* was correctly classified as low risk by our system, based on a confidence score of 5% assigned by AbuseIPDB (Fig. 9). The ICM in our tool sent the classification result to QRadar and logged it in the *Log Activity* module as a low-risk event without triggering an offense. Note that no reports are generated for low-risk IPs. Even though this IP address was classified as low risk, it continues to be systematically monitored because of the possibility of score escalation in future reports. This approach ensures timely reclassification and an appropriate response in the event of malicious activity, reflecting a preventive security strategy aimed at minimizing potential threats at an early stage.

- **IP address**: *117.50.47.222*
- **Score**: *5%*
- **Country**: *CN*
- **Classification**: *Low risk*
- **Last reported**: *May 12, 2025, 7:02:18 AM*

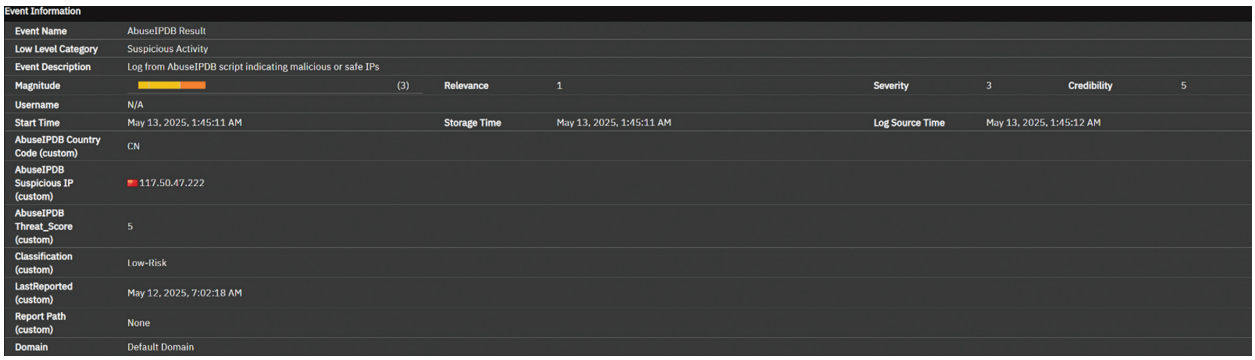

Fig. 9. QRadar's log of low-risk IP 117.50.47.222 (source: created by the authors)

7. CONCLUSION AND FUTURE DIRECTIONS

This paper demonstrates the feasibility and effectiveness of integrating the AbuseIPDB threat intelligence platform with IBM QRadar to enhance the automated analysis of threats and the response to incidents. Our proposed solution embeds a real-time verification mechanism within the SIEM framework, streamlining the detection, classification, and documentation of suspicious IP addresses. The integration is implemented using the ICM, which listens for Syslog messages, extracts IP addresses, and checks their reputation via the AbuseIPDB API. This approach allows the automated classification of threats, avoiding a reliance on manual processing and reducing false positives. Tests confirmed that the integration effectively identifies high-risk IP addresses and enriches event logs with trusted reputation data. The system also generates analytical reports that help security analysts make decisions. Furthermore, this study demonstrates QRadar's flexibility in gathering and analyzing structured data, making it particularly suitable for dynamic security environments that need real-time responsiveness and detailed documentation.

In conclusion, this paper presents a practical model for enhancing SIEM platforms by integrating external threat intelligence. The proposed approach improves organizational readiness against evolving cyber threats. However, our proposed integration approach focuses on analyzing IP addresses and does not incorporate other threat indicators, such as domain names or malware signatures. Additionally, the system relies solely on data from AbuseIPDB, but its effectiveness could be enhanced by integrating additional threat intelligence feeds. Future research directions include (1) expanding threat precision by incorporating threat indicators, such as domain names and file hashes, in addition to IP addresses, to enhance analytical depth, (2) integrating multiple threat intelligence sources, including platforms like VirusTotal and IBM X-Force Exchange, to enable multi-source correlation and improve classification accuracy, (3) incorporating User and Entity Behavior Analytics (UEBA) capabilities into the system to facilitate the detection of anomalous behaviors and advanced persistent threats, (4) enhancing the alerting mechanism within the IBM QRadar platform to support multilevel alert generation, based on the confidence scores and the temporal frequency of the incident reports, (5) assessing integration performance in large-scale environments, such as governmental or financial institutions, to evaluate robustness under high-volume data conditions, and (6) applying machine-learning techniques to improve threat classification accuracy and reduce false positives through advanced behavioral and technical analysis.

8. REFERENCES:

[1] A. Kuzior, I. Tiutiunyk, A. Zielińska, R. Kelemen, "Cybersecurity and Cybercrime: Current Trends and Threats", Journal of International Studies, Vol. 17, No. 2, 2024, pp. 220-239.

[2] A. Tariq, J. Manzoor, M. A. Aziz, Z. U. A. Tariq, A. Masood, "Open Source SIEM Solutions for an Enterprise", Information & Computer Security, Vol. 31, No. 1, 2022, pp. 88-107.

[3] D. Sim, H. Guo, L. Zhou, "A SIEM and Multiple Analysis Software Integrated Malware Detection Approach", Proceedings of the IEEE International Conference on Service Operations and Logistics, and Informatics, Singapore, 11-13 December 2023, pp. 1-7.

[4] T. Owen, "Threat Intelligence & SIEM", Lewis University, Master Thesis, 2014.

[5] J. Smeriga, "Integration of Cisco Global Threat Alert to 3rd Party Product", Masaryk University, Faculty of Informatics, Brno, Master Thesis, 2022.

[6] N. R. Tulcidas, "Event Correlation in Ciências", Universidade de Lisboa, Faculdade de Ciências, Departamento de Informática, Lisbon, Master Thesis, 2024.

[7] A. Esseghir, F. Kamoun, O. Hraiech, "AKER: An Open-Source Security Platform Integrating IDS and SIEM Functions with Encrypted Traffic Analyt-

ic Capability", Journal of Cyber Security Technology, Vol. 6, No. 1-2, 2022, pp. 27-64.

[8] S. K. Bhatt, P. K. Manadhata, L. Zomlot, "The Operational Role of Security Information and Event Management Systems", IEEE Security & Privacy Magazine, Vol. 12, No. 5, 2014, pp. 35-44.

[9] M. Bada, S. Creese, M. Goldsmith, C. Mitchell, E. Phillips, "Computer Security Incident Response Teams (CSIRTs): An Overview", Global Cyber Security Capacity Centre, University of Oxford, Technical Report, 2014.

[10] G. González-Granadillo, S. González-Zarzosa, R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", Sensors, Vol. 21, No. 14, 2021, p. 4759.

[11] O. Podzins, A. Romanovs, "Why SIEM is Irreplaceable in a Secure IT Environment?", Proceedings of the IEEE eStream Conference, Riga, Latvia, 25 April 2019, pp. 1-5.

[12] M. Sheeraz, M. A. Paracha, M. U. Haque, M. H. Durad, S. M. Mohsin, S. S. Band, A. Mosavi, "Effective Security Monitoring Using Efficient SIEM Architecture", Human-centric Computing and Information Sciences, Vol. 13, No. 17, 2023, pp. 1-18.

[13] D. Šuškalo, Z. Morić, J. Redžepagić, D. Regvart, "Comparative Analysis of IBM QRadar and Wazuh for Security Information and Event Management", Proceedings of the 34th DAAAM International Symposium on Intelligent Manufacturing and Automation, Vienna, Austria, 2023, pp. 96-102.

[14] M. Seppänen, "Methods for Managed Deployment of User Behavior Analytics to SIEM Product", JAMK University of Applied Sciences, Degree Programme in Information and Communications Technology, Jyväskylä, Finland, Bachelor Thesis, 2021.

[15] H. Griffioen, T. M. Booij, C. Doerr, "Quality Evaluation of Cyber Threat Intelligence Feeds", Proceedings of the 18th International Conference on Applied Cryptography and Network Security, Rome, Italy, 19-22 October 2020, pp. 251-270.

[16] V. G. Li, M. Dunn, P. Pearce, D. McCoy, G. M. Voelker, S. Savage, K. Levchenko, "Reading the Tea Leaves: A Comparative Analysis of Threat Intelligence", Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 2019, pp. 739-756.

[17] J. L. Lewis, G. F. Tambaliuc, H. S. Narman, W.-S. Yoo, "IP Reputation Analysis of Public Databases and Machine Learning Techniques", Proceedings of the International Conference on Computing, Networking and Communications, Big Island, HI, USA, 17-20 February 2020, pp. 181-186.

[18] R. Ando, H. Itoh, "Characterizing Combatants of State-Sponsored APT in Digital Warfare by Reported Blocklist Database", International Journal of Computer Science and Network Security, Vol. 22, No. 3, 2022, pp. 541-546.

[19] AbuseIPDB, "IP Address Abuse Checker", www.abuseipdb.com (accessed: 2025)

[20] Cisco Systems, "Cisco Global Threat Alerts", www.cisco.com/security/alerts (accessed: 2025)

[21] Wazuh, "Wazuh: Open Source Security Platform", wazuh.com (accessed: 2025)

[22] M. Roesch and the Snort Team, "Snort: An Open-Source Network Intrusion Detection and Prevention System", www.snort.org (accessed: 2025)

[23] C. Sauerwein, T. Staiger, "Cyber Threat Intelligence Sharing Platforms: A Comprehensive Analysis of Software Vendors and Research Perspectives", University of Innsbruck, Department of Information Systems, Production and Logistics Management & Department of Computer Science, Innsbruck, Austria, Master Thesis, 2021.

[24] T. Hussein, "Deep Learning-based DDoS Detection in Network Traffic Data", International Journal of Electrical and Computer Engineering Systems, Vol. 15, No. 5, 2024, pp. 407-414.

[25] R. Singh, R. Ujjwal, "Intrusion Detection System based on Chaotic Opposition for IoT Network", International Journal of Electrical and Computer Engineering Systems, Vol. 15, No. 2, 2024, pp. 121-136.