International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 1, Issue 5, 2022
DOI: https://doi.org/10.38124/ijsrmt.v1i5.583

Leveraging Threat Intelligence in DevSecOps for Enhanced Banking Security

Ayobami Adebayo[1]

[1]Enugu State University of Science and Technology (ESUT), Nigeria

Publication Date 2022/05/29

Abstract

As cyber threats targeting financial institutions grow more complex and persistent, the integration of threat intelligence into DevSecOps pipelines has emerged as a critical strategy for enhancing security in the banking sector. This study investigates how banking organizations leverage threat intelligence to strengthen proactive defenses, automate risk responses, and ensure regulatory compliance. Using a descriptive quantitative approach and structured questionnaires distributed to 60 IT and cybersecurity professionals across various financial institutions, the study examines the level of awareness, utilization, perceived benefits, and challenges associated with threat intelligence in DevSecOps environments. The results reveal a high level of threat intelligence adoption and strong agreement on its benefits—particularly in early threat detection and automation. However, challenges such as a shortage of skilled personnel, integration complexity, and financial constraints hinder effective implementation. The study concludes by recommending enhanced training, adoption of scalable platforms, improved team collaboration, and the use of AI-driven filtering mechanisms to optimize the impact of threat intelligence in secure DevSecOps workflows.

Keywords*: Threat Intelligence, DevSecOps, Banking Security, Cybersecurity, Continuous Integration, Security Automation, Financial Institutions, AI in Security, Compliance, Cyber Threat Detection.*

I. INTRODUCTION

As financial institutions continue to digitize operations and offer services via web and mobile platforms, the threat landscape in banking has expanded significantly. The banking sector has become a primary target for cybercriminals due to its wealth of sensitive data and financial assets (KPMG, 2021). To counter increasingly sophisticated cyber threats, many organizations have adopted DevSecOps—a methodology that integrates security practices into the DevOps pipeline from the outset of software development. However, securing applications in such dynamic environments requires more than automated testing and code analysis. It demands real-time, contextual threat awareness.

Threat intelligence, defined as evidence-based knowledge about existing or emerging threats, plays a crucial role in anticipating, detecting, and mitigating cyberattacks (Husák et al., 2021). When integrated into DevSecOps workflows, threat intelligence can provide developers, security engineers, and operations teams with actionable insights, enabling preemptive security decisions. This synergy ensures that software is not only secure by design but is also resilient to evolving attack vectors.

In banking, threat intelligence becomes even more critical due to compliance demands, the need for data integrity, and the high impact of security breaches (ENISA, 2020). With real-time intelligence feeds, banks can map vulnerabilities against known threats, prioritize remediation efforts, and adjust policies dynamically based on risk context. Moreover, incorporating threat intelligence fosters a proactive rather than reactive approach to cybersecurity, aligning with the fast-paced and iterative nature of DevSecOps.

Despite its importance, the practical integration of threat intelligence into DevSecOps remains underexplored, particularly in the financial sector. This study aims to examine how threat intelligence is leveraged within DevSecOps pipelines in banking institutions and assess its impact on the security posture of applications. The research investigates the tools, practices, and challenges involved, using data collected from DevSecOps professionals in the banking industry.

Adebayo, A. (2025). Leveraging Threat Intelligence in DevSecOps for Enhanced Banking Security. *International Journal of Scientific Research and Modern Technology*, 1(5), 1–4. https://doi.org/10.38124/ijsrmt.v1i5.583

II. LITERATURE REVIEW

➢ *DevSecOps and Its Evolution in Banking*

DevSecOps, a fusion of development, security, and operations, is an emerging paradigm designed to embed security into every phase of the software development lifecycle (SDLC). Unlike traditional approaches where security is often treated as a post-development step, DevSecOps promotes early detection of vulnerabilities and continuous compliance (Ahmad et al., 2021). In the banking sector, where applications often deal with sensitive financial transactions and user data, this integrated approach is vital for minimizing risks and meeting regulatory requirements (Singh et al., 2022).

➢ *Role of Threat Intelligence in Cybersecurity*

Threat intelligence refers to the collection, analysis, and sharing of data about current or potential threats to information systems (Husák et al., 2021). It can be strategic, operational, or tactical. Strategic intelligence supports long-term planning, operational intelligence aids in decision-making during incidents, while tactical intelligence helps in identifying specific indicators of compromise (IoCs). According to Sillaber et al. (2019), threat intelligence empowers organizations with the foresight to anticipate attacks, thereby reducing the window of vulnerability.

➢ *Integration of Threat Intelligence into DevSecOps*

The integration of threat intelligence into DevSecOps is increasingly viewed as a critical enabler of secure software delivery. As per Mirzoev et al. (2020), threat intelligence can be used to automate threat modeling, generate test cases, and tune security controls dynamically. By feeding real-time intelligence into CI/CD pipelines, organizations can improve vulnerability management and reduce false positives. Moreover, threat data can inform access control policies, container security configurations, and patch management protocols (Yoon et al., 2021).

➢ *Applications in the Banking Sector*

Banking applications are subject to rigorous compliance regulations such as PCI DSS, GDPR, and PSD2, making security automation and intelligence integration crucial. According to Alshamrani et al. (2020), threat intelligence in banking helps identify targeted malware, phishing campaigns, and other attack trends specific to financial institutions. A case study by ENISA (2020) revealed that banks using threat intelligence platforms experienced faster incident response times and fewer successful breaches.

➢ *Challenges in Implementation*

Despite its advantages, implementing threat intelligence within DevSecOps is not without challenges. A major barrier is the lack of standardized frameworks for integrating external intelligence feeds into CI/CD tools (Khan et al., 2022). Moreover, the volume of raw threat data can be overwhelming without adequate filtering and prioritization. False positives, irrelevant alerts, and the lack of skilled personnel to interpret threat data are common hurdles (Chadha & Rawat, 2021). Additionally, there is concern about the reliability and timeliness of threat intelligence, especially when shared across organizational boundaries.

➢ *Emerging Tools and Solutions*

To overcome these challenges, a range of tools has emerged that support the automated ingestion and analysis of threat intelligence in DevSecOps environments. Platforms like MISP (Malware Information Sharing Platform), Anomali, and ThreatConnect integrate with CI/CD tools to provide real-time alerting and contextual analysis. AI and machine learning are also being used to improve the relevance and actionability of threat data (Husák et al., 2021). These solutions are evolving to support banking use cases by incorporating regulatory compliance frameworks and specialized threat models.

III. METHODOLOGY

➢ *Research Design*

This study employed a **quantitative research design** using a **descriptive survey method** to investigate how threat intelligence is leveraged in DevSecOps environments within the banking sector. The aim was to gather measurable data on practices, tools, challenges, and benefits associated with the integration of threat intelligence.

➢ *Data Collection Instrument*

The primary instrument for data collection was a **structured questionnaire**, which consisted of closed-ended questions. The questionnaire was divided into five sections:

- Demographic information (job role, experience, organization type)
- Awareness and understanding of threat intelligence
- Current use of threat intelligence tools and platforms
- Perceived benefits and challenges
- Integration practices within DevSecOps pipelines

The questions were designed to elicit responses on a Likert scale (e.g., strongly agree to strongly disagree) and with frequency options (e.g., daily, weekly, never).

➢ *Population and Sampling*

The target population included IT professionals, DevSecOps engineers, security analysts, and system architects working in banking and financial institutions. A **purposive sampling** technique was used to select participants with experience in both DevSecOps and cybersecurity operations. A total of **60 respondents** completed the survey.

➢ *Data Analysis*

Data collected from the questionnaire were analyzed using **descriptive statistics** such as frequencies and percentages. This allowed for the clear presentation of respondents' practices, experiences, and challenges related

to threat intelligence integration in DevSecOps. The results are presented in tables with accompanying interpretations.

➢ *Ethical Considerations*

Participants were informed of the purpose of the study and assured of the confidentiality of their responses. No personally identifiable information was collected, and participation was voluntary. All responses were anonymized before analysis.

➢ Results and Findings

The data collected were analyzed using descriptive statistics (frequency and percentage). The findings are organized into tables with accompanying interpretations.

Table 1 Demographic Profile of Respondents

Demographic Variable	Category	Frequency	Percentage (%)
Job Role	DevSecOps Engineer	18	30.0
	Security Analyst	20	33.3
	System Architect	12	20.0
	Software Developer	10	16.7
Years of Experience	Less than 2 years	9	15.0
	2–5 years	26	43.3
	6–10 years	17	28.3
	Above 10 years	8	13.3
Organization Type	Commercial Bank	24	40.0
	Microfinance Institution	12	20.0
	Fintech	14	23.3
	Regulatory/Compliance Agency	10	16.7

The majority of respondents were either DevSecOps engineers or security analysts with 2–5 years of experience, mostly working in commercial banks and fintech institutions. This aligns with the study's focus on experienced professionals in banking technology and security.

Table 2 Awareness and Usage of Threat Intelligence Tools

Statement	Yes	%	No	%
Aware of threat intelligence platforms	56	93.3	4	6.7
Currently using threat intelligence in DevSecOps	48	80.0	12	20.0
Organization subscribes to external threat intelligence feeds	40	66.7	20	33.3

High awareness (93.3%) and active use (80%) of threat intelligence indicate that banking professionals recognize the importance of threat data. However, one-third of organizations do not subscribe to external threat feeds, suggesting budget or policy constraints.

Table 3 Perceived Benefits of Integrating Threat Intelligence

Benefit Identified	Frequency	Percentage (%)
Early threat detection and prevention	52	86.7
Enhanced security automation	45	75.0
Improved compliance with regulations	40	66.7
Reduced incident response time	38	63.3
Real-time vulnerability mapping	41	68.3

The top perceived benefit is early detection of threats (86.7%), followed by better security automation (75%). These responses affirm the importance of intelligence-driven decision-making in DevSecOps for proactive banking security.

Table 4 Challenges in Integrating Threat Intelligence

Challenge	Frequency	Percentage (%)
Lack of skilled personnel	37	61.7
Integration complexity with CI/CD pipelines	35	58.3
High cost of threat intelligence platforms	30	50.0
Overload of irrelevant threat data (false positives)	28	46.7
Poor internal communication between Dev and SecOps	25	41.7

The biggest challenge reported was the **lack of skilled personnel** (61.7%), followed closely by **integration complexity**. These findings suggest that while tools are available, human resource limitations and system complexity hinder optimal implementation.

IV. CONCLUSION

The study investigated the integration of threat intelligence into DevSecOps practices within the banking sector, focusing on the awareness, usage, benefits, and challenges encountered by IT professionals. Findings revealed a high level of awareness and usage of threat intelligence platforms among banking security personnel, particularly DevSecOps engineers and security analysts. Respondents overwhelmingly acknowledged the value of threat intelligence in enabling early threat detection, automating security operations, and ensuring compliance with regulatory standards.

However, the research also highlighted key challenges, including a shortage of skilled personnel, integration complexity, and financial constraints. These barriers threaten the scalability and efficiency of threat intelligence programs, especially in smaller or less technologically mature banking institutions. Therefore, although the technical benefits of integrating threat intelligence into DevSecOps are well recognized, practical implementation remains uneven across the sector.

The results of this study emphasize that for banks to remain resilient in the face of evolving cybersecurity threats, there must be not only technological investment but also organizational readiness, skilled manpower, and strategic alignment between development, security, and operations teams.

RECOMMENDATIONS

- *Upskill Personnel in Cyber Threat Intelligence (CTI):*

Banking institutions should invest in continuous training programs and certifications for DevSecOps and cybersecurity professionals to bridge the skills gap in handling threat intelligence platforms and tools.

- *Adopt Scalable Threat Intelligence Tools:*

Organizations should prioritize solutions that are cloud-native, API-driven, and compatible with DevOps toolchains to ease the integration of threat intelligence into existing CI/CD pipelines.

- *Encourage Cross-functional Collaboration:*

Breaking down silos between development, operations, and security teams is critical. DevSecOps success depends on a shared understanding of threat models and mitigation strategies across disciplines.

REFERENCES

[1]. Ahmed, S. H., Yousaf, F., & Abbas, R. (2022). *A review on DevSecOps: Integrating security into DevOps*. IEEE Access, 10, 4542–4559.

[2]. Chhetri, S. R., Rashid, A., & Williams, L. (2020). *Security integration in DevOps: Strategies and empirical observations*. In 2020 IEEE/ACM 42nd International Conference on Software Engineering Workshops (ICSEW), 142–149.

[3]. Javed, M. A., & Abbas, A. (2022). *AI-enabled security orchestration for DevSecOps in the financial sector*. Journal of Network and Computer Applications, 200, 103321.

[4]. Khan, R., Ahmed, R., & Ahmad, N. (2021). *A framework for integrating cyber threat intelligence into DevSecOps pipelines*. International Journal of Information Security Science, 10(1), 45–56.

[5]. Mailloux, L. O., & Kerr, P. (2022). *Transforming security operations with real-time threat intelligence*. Cybersecurity Journal, 5(2), 89–103.

[6]. Mirkovic, J., & Reiher, P. (2021). *Understanding and leveraging cyber threat intelligence in financial IT infrastructure*. ACM Computing Surveys, 54(7), 1–35.

[7]. Sharma, P., & Bhardwaj, A. (2020). *DevSecOps model for financial organizations to mitigate cyber threats*. Procedia Computer Science, 167, 2417–2424.

[8]. Yaqoob, I., Salah, K., Imran, M., & Al-Fuqaha, A. (2022). *Blockchain and AI for cybersecurity and compliance in banking ecosystems*. Future Generation Computer Systems, 135, 220–234.