RESEARCH ARTICLE OPEN ACCESS

Threat Intelligence Integration in DevOps for Fintechs Security

Anirudh Mustyala
Software Engineering, Plano - Texas
Email: anirudhmusthyala@gmail.com

--*************************---------------------------------

Abstract :

The DevOps model is integral in facilitating fast development of fintech applications and infrastructures. However, due to focus on delivery speed and the lack of security culture in the model, applications churned out by DevOps teams are susceptible to vulnerabilities. Fintech companies can enhance the efficacy of DevOps teams to develop secure systems by assimilating various practices in the paradigm. Threat intelligence is one of the unique strategies DevOps can incorporate to enhance the security of their applications. This document discusses threat intelligence and how it can be integrated with DevOps to enhance fintech security.

Keywords: DevOps, Data, Infrastructure,Fintech

--*************************---------------------------------

I. INTRODUCTION

The COVID-19 pandemic reshaped the financial sector. The introduction of social distancing guidelines and the push for digital currencies to contain the spread of the virus impelled people across the globe to embrace fintech services. Since the advent of COVID-19, fintech companies have tripled their services to meet the growing demand. The sector has also had to deal with the need to rapidly evolve its services to match customers' changing needs. The necessity to quickly release new features, innovate timely, and offer uninterrupted service to customers has pushed many fintech companies to embrace DevOps. According to Relevant Software (2022), 91 percent of fintech firms have assimilated the DevOps model.

Though DevOps is helping fintech companies to innovate quickly and evolve, A Gartner study (2019) found that 75 percent of organizations that adopt DevOps fail to realize their expectations. Though failure to achieve intended DevOps goals is often associated with issues around organizational learning and change, it can also be attributed to the inability of the DevOps model to develop infrastructure that consistently safeguards fintechs from cyber risks. According to a report published in Infosecurity Magazine (2018), the DevOps model has been producing more insecure applications than ever before. According to the report, the tendency of DevOps teams to build insecure applications is attributable to lagging adoption of security in DevOps models. The agency further notes that over 70 percent of current software contains reusable code. Code reusability provides an ideal mechanism for spreading cyber threats across different company networks. Other factors contributing to DevOps producing unsafe software are the lack of security culture in DevOps teams and the failure of engineers to analyze potential risks and remediate them proactively.

In an attempt to increase the safety of the DevOps model, engineers are starting to incorporate various security mechanisms in the paradigm. Threat intelligence is one of the novel approaches engineers incorporate in DevOps to enhance the security of applications developed via the DevOps model. This piece of writing discusses threat intelligence and how DevOps teams use it to enhance the security of fintech infrastructures.

II. BODY

Threat intelligence

Cyberspace is full of actors actively looking for vulnerabilities to exploit in online systems. These actors exploit strategies such as zero-day exploits, malware, denial of service attacks, man-in-the-middle attacks, and phishing attacks. Besides these strategies, attackers are unswervingly looking for new approaches and avenues to breach cyber systems. Though developers install all the necessary security protocols to fortify company infrastructures against attacks, it is practically impossible to effectively protect against all known and emerging threats. Consequently, there is a need for threat intelligence. Threat intelligence is the collection of evidence-based information about cyber threats, which is organized, analyzed, and used by cybersecurity experts to enhance the security of cyber systems (Bromiley, 2016). Threat intelligence information entails mechanisms attackers use to infiltrate networks, the impact of different attacks on businesses, how to detect the attacks, and advice on defending against the threats. Threat intelligence enables fintech IT teams to keep at par with the changing cybersecurity landscape and evolving threats. Some of the well-known sources of threat intelligence include;

- ***Clear web***: These are sources that are accessible to conventional search engines. They include social media platforms, company press releases, commercial online journals, and open news outlets.
- **Deep web**: These are websites and databases not directly accessible by search engines. These sources are usually not indexed by traditional search engines, making them difficult to access directly. Deep web sources are usually secured by login pages, and some are only accessible to premium users.
- **Dark Web**: The dark web is a rich source of threat intelligence information. Virtually all attack tools and techniques are traded and shared within hacker communities in the dark web. A dark web is an overlay of the internet that can only be accessed via special tools.

Importance of threat intelligence

The primary role of threat intelligence is to collect information about existing and emerging cyber threats and help security experts protect against them. Threat intelligence reveals information about adversaries, such as their motives, tactics, techniques, and procedures (Almohannadi et al., 2018). This information may also help security teams better understand attackers' decision-making process. The C-suit may also use Insights from threat intelligence when making critical decisions such as security budgeting and choosing ideal IT infrastructure for the organization.

Types of Threat Intelligence

There are different types of threat intelligence. While some types are high-level non-technical information about threats, others are detailed technical information about particular threats. Varying types of threat intelligence are used differently and are meant for different consumers. Here is a summary of the main classes of threat intelligence.

- ***Strategic:*** This is high-level information that contextualizes threats. It is non-technical and mostly consumed by high-level officials such as board of directors. Strategic threat intelligence is primarily used in high-level decision-making. For example, fintech directors may use strategic intelligence when approving security budgets or analyzing proposed IT infrastructure.
- ***Tactical:*** This is technical information about threats used by cybersecurity experts to detect and respond to threats. Tactical threat intelligence mainly focuses on indicators of compromise (IoC), such as emails associated with phishing, hashes related to malware, and IP addresses associated with cyber attackers. Tactical intelligence is processed to filter false positives.
- ***Operational threat intelligence***: Also called technical threat intelligence, operational intelligence helps security teams anticipate and prevent future attacks. Operational intelligence outlines tactics, techniques, procedures, and behaviors of probable adversaries. Security teams leverage operational threat intelligence to identify potential attackers and install necessary security controls to protect their infrastructure.

Integrating threat intelligence into DevOps

Integrating threat intelligence in the DevOps model enables DevOps teams to predict, detect, and respond to cyber threats in a timely and cost-effective manner. DevOps and threat intelligence integration facilitates vulnerability detection and patch management automation, allowing DevOps teams to focus on more critical roles. To successfully integrate threat intelligence into DevOps, the teams must have a configuration management server, vulnerability scanning system, firewall management systems, and a threat feed. With these resources, DevOps teams can integrate threat intelligence through the threat intelligence lifecycle, which consists of six steps. These steps include;

- ***Requirements:*** The requirements stage is threat intelligence's first and most vital phase. In this stage, DevOps teams agree on the specific threats they want to investigate and the goals and objectives the operation should achieve. In the fintech sector, the goals might be discovering adversaries targeting fintech firms and their motives, the attack surface, and the specifications that should be adopted to thwart the risks.
- ***Data Collection***: As soon as the requirements are defined and the goals are specified, the next step is launching data collection operations. The data collection involves exploring traffic logs, open source data avenues, social media, the dark web, relevant forums, and industry experts. To get threat intelligence information pertinent to the fintech sector, it is noble for DevOps teams to leverage feeds that specialize in the financial industry. To access a wide range of information on the web, the data collection phase is orchestrated using artificial intelligence tools. AI tools are capable of scrapping the net and finding relevant threat intelligence information within seconds (Battina, 2021).
- **Processing:** Collected data must be processed into suitable formats. The processing phase involves further

evaluation of data and filtering out irrelevant materials, translating materials into desired language, decrypting files, and organizing data points into spreadsheets. Processing large junks of data manually can be time-consuming and laborious. In DevOps, processing can also be automated using AI-based tools.

- **Analysis:** This is where actionable insights are retrieved from collected data. The analysis is executed based on the goals and objectives established in the requirements phase. The team organizes the insights into actionable items and valuable recommendations for the consumers of the information. The analysis phase is also conducted by AI tools. However, some processes, such as recommendations, may be done manually.
- **Dissemination**: This stage entails the team translating the analysis into a consumable format and forwarding it to the intended recipients of the information. The format and complexity of the information depend on the intended audience. If the audience is the C-suit, then the presentation format should be simple and precise – no technical jargon and presented as a one-page report, PPT, or a short slide deck.
- **Feedback:** This is the last stage of the threat intelligence lifecycle. The recipients of the report give their thoughts about the report. This may include requesting adjustments to the report or providing guidance on how they may wish to receive similar reports in the future.

III. CONCLUSION

The DevOps model is integral in facilitating fast development of fintech applications and infrastructures. However, due to focus on delivery speed and the lack of security culture in the model, applications churned out by DevOps teams are susceptible to vulnerabilities. Fintech companies can enhance the efficacy of DevOps teams to develop secure systems by assimilating various practices in the paradigm. Threat intelligence is one of the unique strategies DevOps teams can assimilate to enhance the security of their application. Threat intelligence not only gives DevOps engineers information about existing and emerging threats but also encourages the C-suit to support security initiatives through appropriate budget allocations. In simpler terms, threat intelligence integration with DevOps streamlines cyber security initiatives from the top management to DevOps engineers. Fintech companies seeking to enhance their cybersecurity posture can start by integrating threat intelligence into their DevOps models.

REFERENCES

Almohannadi, H., Awan, I., Al Hamar, J., Cullen, A., Disso, J. P., & Armitage, L. (2018, May). Cyber threat intelligence from honeypot data using elasticsearch. In *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)* (pp. 900-906). IEEE.

Battina, D. S. (2021). Ai and devops in information technology and its future in the united states. *INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT), ISSN*, 2320-2882.

Bromiley, Matt. "Threat intelligence: What it is, and how to use it effectively." *SANS Institute InfoSec Reading Room* 15 (2016): 172.

Gartner (2019), The secret to DevOps Success. Retrieved From: https://www.gartner.com/smarterwithgartner/the-secret-to-devops-success

InfoSecurity Magazine (2019), DevOps Producing More Insecure Apps Than Ever. Retrieved From: https://www.infosecurity-magazine.com/news/devops-producing-more-insecure/

Relevant Software (2022), **Fintech and DevOps: Does Your Company Need a DevOps Strategy in 2023? Retrieved From:** https://relevant.software/blog/fintech-and-devops/