Automating Threat Intelligence for SDL

Raghudeep Kannavara
Intel Corporation
Hillsboro, OR, USA

Jacob Vangore
Olivet Nazarene University
Bourbonnais, IL, USA

William Roberts
Olivet Nazarene University
Bourbonnais, IL, USA

Marcus Lindholm
Intel Corporation
Santa Clara, CA, USA

Priti Shrivastav
Intel Corporation
Santa Clara, CA, USA

The frequency of vulnerability disclosures and the sophistication of security attacks have progressively increased in recent years. Consequently, to build more secure products and services while addressing security compliance requirements during the development stage, the Security Development Lifecycle (SDL) was introduced. SDL integrates with the product lifecycle process, i.e., product definition, design, development and validation, in order to ensure that the product meets security and privacy requirements. Nevertheless, in order to execute a well-informed SDL, i.e., to architect, design, develop, test and deploy a product or a service meeting the desired security objectives, Threat Intelligence (TI) is a pre-requisite. The purpose of threat intelligence in the context of SDL is to help development teams understand the security risks, such as design or component weaknesses, vulnerabilities, exploits, attacker motives and techniques, pertinent to their products or services, and enable them to effectively address these security risks during Product Development Lifecycle and even after deployment. TI is the set of data collected, assessed and applied regarding emerging security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators [1] [2]. This set of data enables the stakeholders to arrive at informed decisions when managing security risks. It also drives mitigations to counter attack vectors used by threat actors, thereby protecting the assets. This translates to protecting a company's brand, business and customers.

A threat driven approach to SDL enables a product development team to be proactive in understanding the security risks associated with the underlying technologies in use, thus enabling the architecture and implementation of mitigations in the early phases of the product development lifecycle. Whereas a vulnerability driven approach to manage security risks is reactive and forces the product team to focus on managing specific vulnerabilities, rather than addressing larger scale threat scenarios and patterns [4].

There are numerous high quality open source or publically available threat feeds that are constantly kept updated by the security community with emerging threats and latest vulnerability disclosures. These publically available threat feeds are commonly called open source intelligence (OSINT). Much of the information needed for threat intelligence extraction can be collected from these open source threat feeds. It has been reported that in mixed-source reports (i.e. information from a number of different sources, including OSINT and other sources), open source intelligence regularly provides 80% of the content [3]. While open source threat feeds include National Vulnerability Database (NVD), twitter feeds, security blogs, security conference presentations and publications, security advisories, white papers and so on, other sources include commercial threat feeds, data from industry partners, human intelligence, internal or secret information etc.

Since the volume of threat information sources is overwhelmingly vast and diverse, manual analysis to distill intelligence from raw data is not feasible. Hence, automation is key to any successful threat intelligence initiative. While manual analysis of threat data to gather intelligence is critical to informed decision making, automation makes it much easier for stakeholders to arrive at these decisions. In our survey, we found that there are numerous readily available solutions to automate threat intelligence research and management to secure an organization's IT infrastructure. For example, network intrusion detectors or tools focusing on malware, botnets or phishing campaigns. On the other hand, there exists a lack of readily deployable solutions that primarily focus on threat intelligence pertinent to a product SDL. To address this shortcoming, in our poster session, we highlight the importance of a threat intelligence driven SDL to improve product security assurance and explain how strategic threat intelligence can be incorporated in the different phases of SDL. We will also present our automated solution, namely Threat Miner for SDL that leverages Open Source Intelligence (OSINT) to deliver product specific threat indicators designed to strategically inform the SDL while continuously monitoring for disclosures of relevant potential vulnerabilities during product design, development, and beyond deployment.

Furthermore, we will discuss the requirements, architecture and deployment of our solution. We will share key learnings from having deployed Threat Miner for SDL in our Business Unit at Intel Corp. These learnings include Best Known Methods on how we have integrated Threat Miner for SDL in assessing product security risks, hardening product architecture and design, verifying implementation and managing product release and survivability. Moreover, we have open sourced the code repository for Threat Miner for SDL. During our poster session, we will provide the audience with details on how to access and install the open source version of Threat Miner for SDL.

REFERENCES

[1] M. Bromiley, "Threat Intelligence: What It Is, and How to Use It Effectively," SANS Whitepaper, September 2016.

[2] "Threat Intelligence: What is it, and How Can it Protect You from Today's Advanced Cyber-Attacks?," Gartner Files, Webroot Publication.

[3] R. D. Steele, "Open Source Intelligence: What Is It? Why Is It Important to the Military?," International Public Information Clearinghouse, Open Source Solutions, Inc.

[4] M. Muckin, S. C. Fitch "A Threat-Driven Approach to Cyber Security," Lockheed Martin Corporation.