A Comparative Study between Azure Sentinel and Splunk.

Supervisor – Dr Oisin Cawley

Bhupal Gurung – C00291390@setu.ie | M.Sc. in Cybersecurity, Privacy and Trust

Introduction

Microsoft Sentinel is a next-generation security solution based on artificial intelligence and machine learning that is entirely cloud-based and it is a Microsoft's native SIEM. Using Microsoft Sentinel, organisations can identify and eliminate threats more quickly.

For security, IT, and DevOps, Splunk is a "data-to-everything" security platform. Features including investigation and forensics, unified security operations, automation and orchestration, security analytics and SIEM, and investigation and forensics are all included in the Splunk Security Cloud. Big data and artificial intelligence are also utilised by Splunk, an all-in-one security solution, to identify and lessen threats (R2 Unifoed Technologies, n.d.).

Research Questions

- Research question 1 – What are the prospective challenges and restrictions related to geolocation mapping in SIEM systems and suggest solutions?
- Research question 2 – How well the IP geolocation mapping improves Security Information and Event.
- Research question 3 – How this research compares azure sentinel and Splunk's features, functions, and performance in relation to a geolocation mapping implementation for online threat detection?

Early Indicators

- Ethical factors like data privacy are constantly updating and organisations needs to be updated to the current standard while dealing with IP.
- When selecting a SIEM solution for your company, there are several things to consider, such as licencing, functionality, budget, and more.
- Splunk offers a wide range of functionalities required to monitor events in real-time, making it more appropriate for larger enterprise organisations that may have previously invested in Spunk Core. As an alternative, companies looking for a real Extended Detection & Response (XDR) solution with AI-driven analytics focus on threat detection might be better served by Microsoft Sentinel (2 Steps Team, 2023).
- .

References

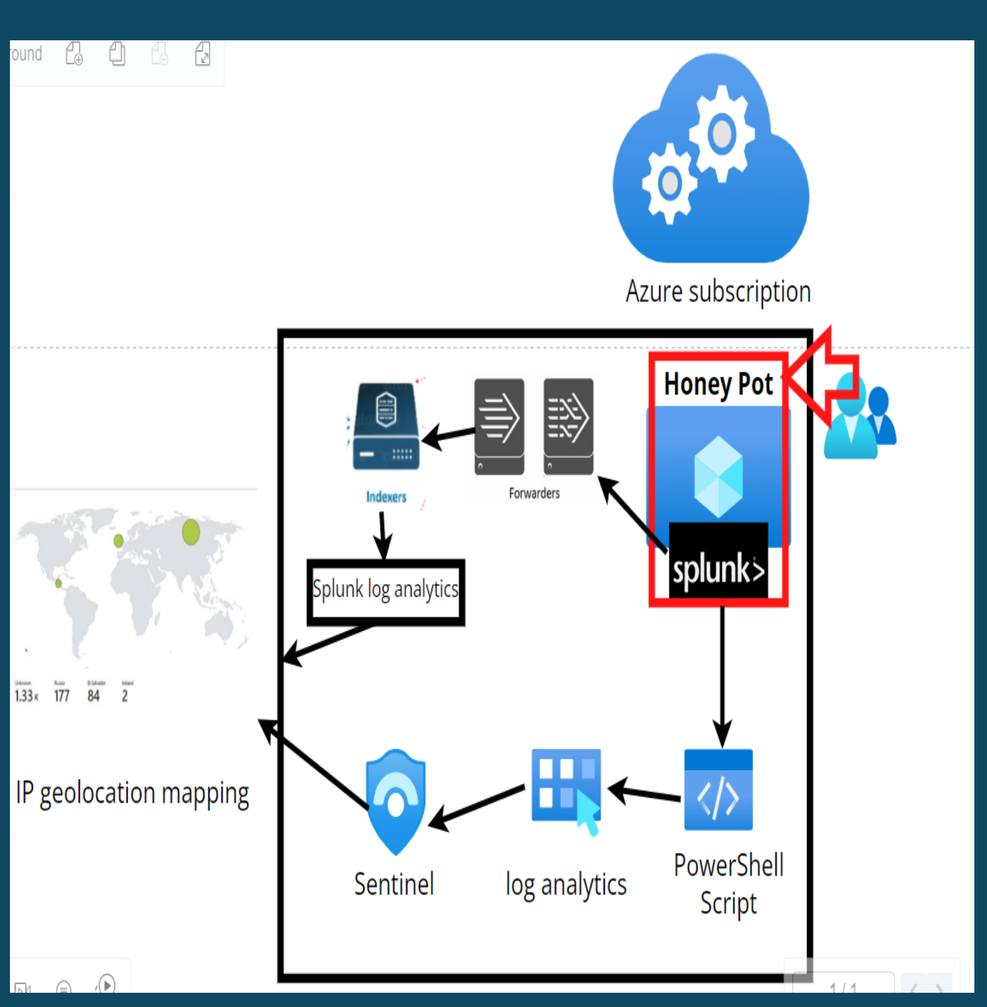
R2 Unifoed Technologies, n.d. Comparing Microsoft Sentinel vs. Splunk. [Online] Available at: https://blog.r2ut.com/comparing-microsoft-sentinel-vs.-splunk

[Accessed 04 04 2024].

ps Team. (2023, 01 09). Splunk Monitoring: What is it and How Can You Use it? Retrieved from https://blog.2steps.io/splunk-monitoring-what-is-it-and-how-can-you-use-it

Literature review

- A significant gap in the current body of literature is the lack of a direct comparison of different SIEM systems geolocation mapping functionalities.
- This dissertation seeks to close this gap by highlighting the advantages and disadvantages of Splunk and Azure Sentinel in the context of geolocation mapping for cyber threat detection.
- This dissertation finds out that Splunk offers more option and functionalities to help threat detection in IP geolocation mapping, but it is highly complicated in comparison to Sentinel.
- Sentinel is completely cloud based and easy to implement, which does not require highly qualified engineers to operate.
- Before choosing, this thesis suggests comparing the two systems, carry out proofs of concept, and determine how well their AI and machine learning capabilities match your cybersecurity goals.



Methodology

- Created a honeypot inside azure and installed splunk inside it.
- Trace the IP geolocation of the attacker using splunk enterprise with custom build extract field.
- Traced the IP geolocation of the attacker's PC using sentinel with custom extract field and map the live attack.
- Compared the efficacy and the differences between the two SIEM.