Manasvini Duddukuru

MALWARE INFORMATION SHARING PLATFORM

Abstract:

This reports highlights the detailed summary of the cyber security tool MISP (Malware Information Sharing Platform), and it focuses on its sustainability for Small and Medium-sized enterprises for developing countries.

SME's usually experience various cyberattacks, however some SME's aren't capable enough to prevent some attacks from occurring and find it difficult to go against these attacks [1]. Hence, researchers have identified that these small and medium-sized enterprises need assistance requiring cyberattacks, and one such solution is the MISP, now known as a threat intelligence sharing platform [1].

Tool Description:

MISP is a cyber security tool, which is known as Malware Information Sharing Platform, and is also widely known as an Open-Source Threat Sharing Platform, where organisations are able to store, share and receive information regarding threats, malware and vulnerabilities [2].

The tool is known to correlate between indicators of threat intelligence, and targeted attacks, any vulnerable information, financial deceptions and any information regarding counter-terrorism [2].

The goal of the tool is to prevent actions that are utilised against targeted attacks, as well as enabling detection about threats and malware [2].

Key Features:

Key features regarding MISP tool include that the tool is able to synchronize events and attributes automatically amongst other different MISP tools [2]. It has an advanced filter functionality which can be utilised to meet the requirements for the sharing policy for different organisations and comprises of an 'attribute level distribution mechanism' and a flexible sharing group space [2].

System Requirements:

The MISP tool system's requirements are modest, and don't require much storage, making it an efficient option for small and medium sized enterprises [3].
It requires a single virtual CPU, 2GB RAM and 8-16 GB memory [3].

Installation Process:

The cyber security tool can be installed on any Linux/GNU device [4].
The installation process for installing MISP can be quite difficult, as there are options to choose from to download MISP, such as on Ubuntu, Docker, and others [4].
As Ubuntu has various versions, there are a separate set of instructions for the installation and manual process, depending on the server of Ubuntu [4]. The tool also requires MariaDB as its database, and the utilisation of SSD's would be efficient [4].

Core Functionalities:

A few core functionalities of the MISP tool:

- They have programmed correlation between indicators and attributes that are from malware, and the engine for correlation includes more advanced options such as CIDR block matching and ssdeep [2].

- It has an effective IoC (Indicator of Compromise), which is a database that enables to save technical and non-technical information about intelligence, incidents, malware models and attackers [2].

- It provides an 'intuitive user-interface' which aids SME's to easily be able to collaborate and create on attributes and events [].

Use Cases and Practical Applications:

There are a few use cases and practical applications for MISP tool, and these include researching and sharing information, where the tool is quite handy for users to consume the IoC's in an organised manner, and it aids to search through domains and IP address even if they have been indicated malicious [5].

Another scenario includes pushing the IoC to firewalls and intrusion detection systems (IDS's). This allows users to automate features of the organisation's protection methods against threats without the requirement of a manual configuration [5].

Reference:

[1] Haastrecht MV, Golpur G, Tzismadia G, Kab R, Priboi C, David D, Racataian A, Baumgartner L, Fricker S, Ruiz JF, Armas E, Brinkhuis M, Spruit M. A Shared Cyber Threat Intelligence Solution for SMEs. Electronics [Internet]. 2021 November 24 [cited 2024 April 2]; 10: 2913. Available from: https://doi.org/10.3390/electronics10232912

[2] MISP Threat Sharing. MISP Features of MISP, the open-source threat sharing platform. [cited 2024 March 29] Available from: https://www.misp-project.org/features/

[3] MISP Threat Sharing. Sizing your MISP Instance. [cited 2024 March 29] Available from: https://www.misp-project.org/sizing-your-misp-instance/

[4] MISP Threat Sharing. Download and Install MISP. [cited 2024 March 29] Available from: https://www.misp-project.org/download/

[5] Postolovski T. What is MISP? The Ultimate Introduction. [cited 2024 April 2] Available from: https://www.cosive.com/blog/what-is-misp-the-ultimate-introduction