

INVESTIGATION INTO THE QUALITY OF OPEN-SOURCE CYBER THREAT INTELLIGENCE

Lee Canning | 2116294 | BSc Networking & Cyber Security

1. INTRODUCTION

Cyber Threat Intelligence helps security professionals detect, triage, and investigate threats and is increasingly seen as a crucial security tool [1]. Official intelligence sources can be inhibitive expensive, however OSCTI can prove to be just as valuable if the intelligence is of sufficient quality and delivered in a timely and efficient manner.

2. AIMS & OBJECTIVES

The aim of the assignment is to conduct an experiment on an OSCTI platform, that could be deployed within DHCW's security portfolio and integrate with SIEM systems to ensure cyber threats are sufficiently identified, analysed, and mitigated

The objectives are to:

- Conduct extensive research and literature reviews of OSCTI.
- Analyse and identify key strengths and weaknesses of current systems.
- Curate and configure OS intelligence feeds.
- Conduct an experiment to measure the quality of the intelligence feeds.
- Offer a conclusion and suggest future work.

3. LITERATURE REVIEW

The literature review explored and critiqued existing literature and research on the emerging trends of threat intelligence, focused on OSCTI. It compares the concerns around OSCTI quality vs CSCTI, trust issues around sharing intelligence, and how that intelligence is sourced and shared.

Key Findings:

- There remains a notable gap in studies measuring the quality of OSCTI, and whether it can provide reliable, quality intelligence.
- The sheer volume of OSCTI can make it difficult to discern actionable intelligence from noise, and that a lack of expertise and knowledge of analysts only emphasises this issue.

4. RESEARCH EXPERIMENT & HYPOTHESIS

To test the quality of OSCTI data, an experiment and research hypothesis was devised.

Independent Variables

Low diversity group: 2-3 generic OSCTI feeds.
High diversity group: 10-12 specialised OSCTI feeds.

Dependent Variable

Number of unique IoCs ingested by the TIP.

Research Hypothesis

"Increasing the number and variety of OSCTI feeds ingested into a TIP will result in a statistically significant increase in the number of unique IOCs detected."

5. DESIGN & IMPLEMENTATION

- Two MISP instances deployed in an MS Azure environment (Ubuntu VMs) to ingest low and high diversity group feeds.
- Python script extracted data from MISP API
- Data exported to MS Excel for statistical analysis

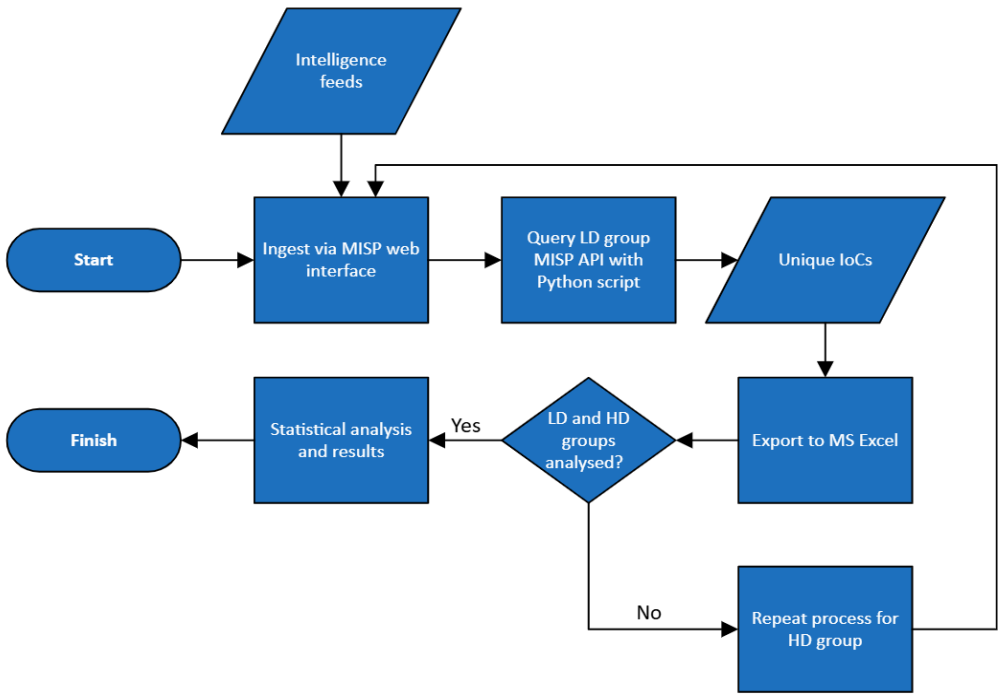


Fig 2: Data flow diagram of lab environment setup.

6. RESULTS & CONCLUSIONS

- Increased diversity of OSCTI feeds = increased volume of IoCs.

The higher diversity group yielded a statistically significant increase in the volume of unique IoCs. However, this also increased the fluctuation in the total volume of attributes ingested.

Low diversity Vs high diversity daily total IoCs

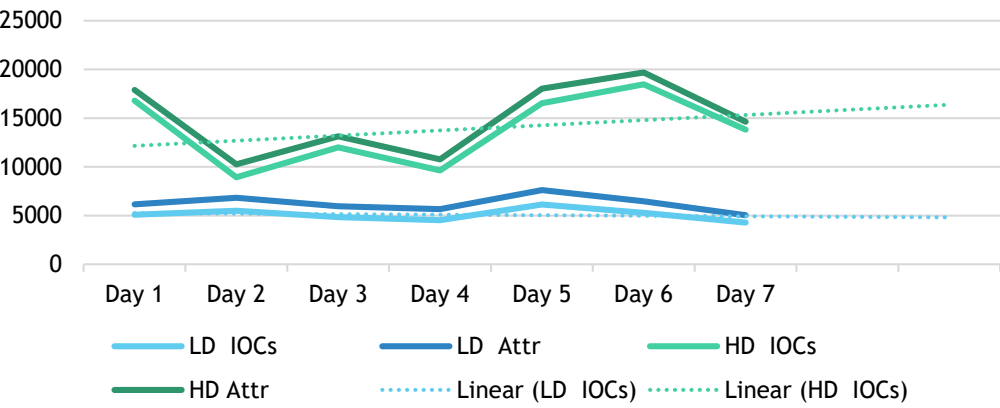


Fig 1: Line graph comparing low and high diversity groups with trendlines.

	F1	F9	F13	F33	F35	F41	F49	F73	F74	F80	F81	F84	F89	F93	F94	F97
Feed #1 CIRCL OSINT Feed	-	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%
Feed #9 ip-block-list - snort.org	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Feed #13 OpenPhish url list	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Feed #33 VXvault - URL List	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%	0%	0%
Feed #35 http://cybercrime-tracker.net hashlist	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Feed #41 URLHaus Malware URLs	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Feed #49 malsilo domain	0%	0%	0%	0%	0%	0%	-	0%	0%	25%	0%	0%	75%	0%	0%	0%
Feed #73 List of malicious hashes	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	1%	0%	0%	0%
Feed #74 Shreshta: Newly Registered domain names(NRD) - 1 week (Community policy feed)	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%
Feed #80 Threatview.io - Domain Blocklist	1%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	56%	0%	0%	0%
Feed #81 Threatview.io - MD5 Hash Blocklist	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%
Feed #84 Threatview.io - SHA File Hash Blocklist	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%
Feed #89 ThreatFox IOCs	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	-	0%	0%	0%
Feed #93 ISC IP + Hostnames	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	-	63%	56%	
Feed #94 ISC Dump	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	9%	
Feed #97 CI Army	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	69%	-	

Fig 3: MISP overlapping feeds matrix.

REFERENCES

[1] A. B. Michael Clark, "How to Use Threat Intelligence for Security Monitoring and Incidence Response," Gartner, Stamford, CT, 2020.

7. REFLECTIONS & FUTURE WORK

- Hypothesis validated.
- Aims & objectives met.
- OSCTI can prove beneficial if feeds are curated to suit the target organisation.
- Conducting the experiment over a longer period will provide more basis for statistical analysis.
- Deploying MISP instances on DHCW Azure environment will allow for integration with MS Sentinel and curated OSCTI feeds such as NCSC's TISP, and MS Free TI Feeds.
- More research to be conducted into MISP correlation to get a better insight into quality.
- More research to be conducted into OSCTI vs CSCTI to discover more benefits.

DHCW: Digital Health & Care Wales; **OSCTI:** Open-Source Cyber Threat Intelligence; **CSCTI:** Closed Source Cyber Threat Intelligence; **IoC:** Indicator of Compromise; **MISP:** Malware Information Sharing Platform; **TIP:** Threat Intelligence Platform; **SIEM:** Security Information and Event Management