

**ENHANCING CYBER DECEPTION FOR MS SQL: INTEGRATING AN
OPENCANARY HONEYPOT WITH A REAL DATABASE FOR ATTACKER
PROFILING**

By

Ardhi Atmaja Karo Karo

22451027

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

Revision after the Thesis Defense on August 12, 2025

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.



Ardhi Atmaja Karo Karo

Student

25-8-2025

Date

Approved by:



Dr. Ir. Charles Lim, M.Sc., B.Sc.

Thesis Advisor

®

25-8-2025

Date



Kalpin Erlangga Silaen, S.Si., M.Kom.

Thesis Co-Advisor

23-8-2025

Date

Dr. Ir. Maulahikmah Galinium, S.Kom.,
M.Sc

Dean of Faculty of Engineering and
Information Technology

Date

Ardhi Atmaja Karo Karo

ABSTRACT

ENHANCING CYBER DECEPTION FOR MS SQL: INTEGRATING AN OPENCANARY HONEYPOT WITH A REAL DATABASE FOR ATTACKER PROFILING

By

Ardhi Atmaja Karo Karo

Dr. Ir. Charles Lim, M.Sc., B.Sc. , Advisor

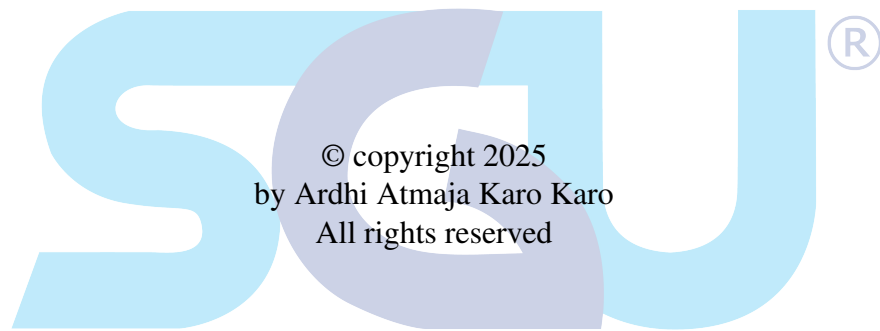
Kalpin Erlangga Silaen, S.Si., M.Kom. , Co-Advisor

SWISS GERMAN UNIVERSITY



The rapid growth of global data emphasizes the critical need for robust, scalable, and secure database systems. Among these, Microsoft SQL Server (MS SQL) stands out as a widely used yet frequently targeted platform for cyberattacks, exposing organizations to risks such as data breaches and operational disruptions. This study leverages deception technologies, employing OpenCanary and Dionaea honeypots to emulate MS SQL environments and gather actionable intelligence on attacker behavior. By analyzing enriched datasets and visualizing attack patterns, the research reveals geographic origins, tools, and attacker profiles, providing valuable insights to inform targeted defense strategies and enhance database security.

Keywords: Honeypot, Microsoft SQL Server, MS SQL, Enrichment, OpenCanary



DEDICATION

I would like to dedicate this research project to my God, my family, my beloved country Indonesia and my second home where I grow in knowledge, Xynexis Group.



ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Dr. Ir. Charles Lim, M.Sc., B.Sc. and Mr. Kalpin Erlangga Silaen, S.Si., M.Kom. as my Thesis advisor. It is because of their priceless contributions that this thesis proposal and the whole research project can arrive at this point. I can't thank you enough for the time that already taken from you for me to make this thesis done.

I would like to thank all of my direct supervisor, my team at work and my friends especially Batch 34 MIT SGU for their companionship, and to the countless number of people who have helped me throughout this research project, either directly or indirectly.



Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	4
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	9
LIST OF FIGURES	10
LIST OF TABLES	11
LIST OF PUBLICATIONS	12
COMMERCIAL TECHNICAL REPORT	13
1. INTRODUCTION	16
1.1 Background	16
1.2 Research Problems	18
1.3 Research Objectives	19
1.4 Research Questions	20
1.5 Hypothesis	20
1.6 Research Scope and Limitation	20
1.6.1 Scope	20
1.6.2 Limitations	20
1.7 Contributions	21
1.8 Research Roadmap and Publications	21

1.8.1	First Semester: Initial Research and Conference Publication	21
1.8.2	Second Semester: Practical Implementation and Industry Contribution	22
1.8.3	Third Semester: Enhancing Interaction Through Real MS SQL Database Integration	22
1.8.4	Final Phase: Thesis Completion and Future Work	22
1.9	Thesis Structure	23
2.	LITERATURE REVIEW	24
2.1	Digital Transformation	24
2.2	Database	25
2.2.1	Logical Foundations and Practical Implications	26
2.2.2	Early Relational Systems: INGRES and System R	27
2.2.3	Object-Relational Innovation: Postgres	28
2.2.4	In-Memory OLTP Systems: H-Store	28
2.2.5	Cloud-Based Relational Services: Relational Cloud	29
2.2.6	OLTP vs. OLAP in the MSSP Context	29
2.3	Microsoft SQL Server	30
2.3.1	SQL Server Security Model and Attack Surface	31
2.3.2	Tabular Data Stream (TDS) Protocol	31
2.3.3	Operational Risk and Containment in Real DB Integration	31
2.4	Cyber Threat	32
2.5	Cyber Defense	33
2.6	Cyber Deception	34
2.6.1	Design Objectives and Threat Model	34
2.6.2	Technique Families for Databases	34
2.6.3	Game-Theoretic Planning	35
2.6.4	Ethics and Legal Considerations	35
2.7	Honeypot	36
2.7.1	Interaction Levels and What They Mean Empirically	37
2.7.2	Containment Without Killing Believability	38
2.7.3	Anti-Fingerprinting for MSSQL Decoys	38
2.8	Evolution of MSSQL-Facing Honeypots	39

2.9	Attacker Profiling	42
2.9.1	Purpose and Scope	42
2.9.2	Data Sources and Features	42
2.9.3	Tool Attribution via Client Interfaces	42
2.9.4	Mapping to MITRE ATT&CK for MSSQL	42
2.9.5	Graph and Sequence Analyses	43
2.9.6	Biases and Limitations	43
2.9.7	Outputs	43
2.10	Previous Studies (Our Group Research)	43
2.11	Previous Studies	45
2.11.1	Critical Synthesis and Implications for the Research Framework	48
3.	RESEARCH METHODS	51
3.1	Research Framework	51
3.1.1	Building Blocks Derived from Chapter 2	51
3.1.2	How the Framework Works (End-to-End Flow)	53
3.1.3	Approach to Enhance Cyber Deception	54
3.2	System Setup	54
3.2.1	System Setup: Real MS SQL Installation, Configuration, Isolation, and Interaction	55
3.2.2	Attacker Access Paths to MS SQL	58
3.3	Data Collection	58
3.4	Data Enrichment	58
3.5	Data Visualization	58
3.6	Analysis	58
3.7	Evaluation and Validation	59
3.7.1	Success Measures for the Deception Design	59
4.	EXPERIMENTS	62
4.1	Experiment Results	62
4.1.1	Experiment Setup	62
4.1.2	System Architecture	63
4.1.3	Request Walkthrough	65

4.1.4	Deception Method Parameters	65
4.1.5	Why a Python Proxy?	67
4.2	Results	68
4.2.1	Data Collection	68
4.2.2	Data Enrichment	69
4.2.3	Data Visualization	69
4.2.4	When and How Attackers Gain Access	70
4.2.5	SQL Commands Executed	70
4.3	Discussions	70
4.3.1	Username	70
4.3.2	Attacker's Profile	71
4.3.3	Attacker's Tools	73
4.3.4	Summary	75
4.3.5	Interpreting Depth & Deception Metrics	75
4.3.6	Interpreting Depth & Deception Metrics (Results)	75
5.	CONCLUSIONS AND RECOMMENDATIONS	77
5.1	Conclusions	77
5.1.1	Achievements vs Targets	77
5.2	Recommendations	78
5.3	Future Works	79
	REFERENCES	88
	A. Source Code	89
	GLOSSARY	98

List of Figures

1.1 Databases with Most Login Attempts (Zdonczyk, 2023)	17
1.2 Fishbone Diagram	18
2.1 The volume of data/information created, captured, copied and consumed worldwide from 2010 to 2025. Statistics from Statista (2021).	25
2.2 Connection to MS SQL Database	30
3.1 Research Framework	51
4.1 System Architecture	63
4.2 Second Phase System Architecture	64
4.3 Top Usernames Used by Attackers.	71
4.4 Top IP Addresses and Countries of Attackers.	72
4.5 Profiling Attackers: Application and Computer Names Used	73
4.6 Mapping Attackers' Tools to Client Interfaces	74
4.7 Distribution of Attackers' Applications	75

List of Tables

2.1 MSSQL honeypots (compact comparison)	41
2.2 Critical Review of Previous Studies	47
4.1 Hardware & Software Specifications	62
4.2 Second Phase Hardware & Software Specifications	63
4.3 Comparison of Data Collected by the MS SQL Service between Dionaea and OpenCanary	71
4.4 Top 10 IP Addresses with Computer Name, Application Name, and Count of Records	73
4.5 Client Interface and Application Used By Attackers	74
4.6 Deception effectiveness metrics.	76
4.7 Top SQL verbs and sensitive procedure attempts (Enhanced).	76
5.1 Targets vs outcomes	78

List of Publications

This chapter provides a record of the research contributions made throughout the academic journey. The listed publication highlights the work conducted in the domain of cybersecurity, focusing on honeypot enhancements and attacker profiling.

1. Enhancing OpenCanary Honeypot to Profile Attackers Behavior on MS SQL

Status: Accepted and Presented

Acceptance Date: December 1st, 2024

Presentation Date: December 11th, 2024

Abstract: The rapid growth of global data emphasizes the critical need for robust, scalable, and secure database systems. Among these, Microsoft SQL Server (MS SQL) stands out as a widely used yet frequently targeted platform for cyberattacks, exposing organizations to risks such as data breaches and operational disruptions. This study leverages deception technologies, employing OpenCanary and Dionaea honeypots to emulate MS SQL environments and gather actionable intelligence on attacker behavior. By analyzing enriched datasets and visualizing attack patterns, the research reveals geographic origins, tools, and attacker profiles, providing valuable insights to inform targeted defense strategies and enhance database security.

This publication represents a significant step toward advancing cybersecurity research. It contributes to the understanding of attacker behaviors and the refinement of defensive security mechanisms, reinforcing the importance of proactive security measures in an MSSP environment.

Commercial Technical Report

PT. NOOSC Security Global (NSG) specializes in providing Managed Security Service Provider (MSSP) solutions, ensuring robust security measures for various clients. As part of NSG's commitment to excellence, a set of technical guidelines has been established to standardize the security configuration, inspection, and implementation of MSSP systems. These guidelines serve as a reference for internal teams and clients, ensuring adherence to industry best practices and regulatory requirements.

Security Configuration for Implementing the MSSP System

Establishing a secure MSSP system requires a structured approach to configuration. The following key aspects must be addressed:

1. Network Security Configuration

- Enforce least privilege access controls for MSSP infrastructure.
- Implement network segmentation to isolate MSSP services from client environments.
- Configure firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and mitigate threats.
- Apply encrypted communication protocols for data transmission.

2. Authentication and Access Management

- Utilize multi-factor authentication (MFA) for all administrative accounts.
- Implement centralized identity and access management (IAM) solutions.
- Regularly review and update access control policies.

3. Logging and Monitoring

- Enable centralized logging with secure storage and access controls.
- Utilize Security Information and Event Management (SIEM) solutions for real-time monitoring.

- Define alerting mechanisms and automated incident response workflows.

4. System Hardening and Patch Management

- Apply vendor-recommended hardening guidelines to all MSSP components.
- Maintain an up-to-date patching schedule for operating systems, applications, and firmware.
- Disable unnecessary services and enforce strict configuration baselines.

5. Data Protection and Compliance

- Implement encryption for data at rest and in transit.
- Enforce data retention policies aligned with regulatory requirements.
- Regularly conduct security assessments and compliance audits.

Checklist for Inspection, Implementation, and Post-Implementation of MSSP Solutions and Systems

To ensure the successful deployment of MSSP solutions, a structured checklist is necessary for each phase of the implementation.

1. Inspection Phase

- Assess client requirements and regulatory compliance needs.
- Conduct a security risk assessment of the existing infrastructure.
- Validate the readiness of network architecture and security policies.
- Review documentation and previous audit reports.

2. Implementation Phase

- Deploy MSSP infrastructure based on approved security configurations.
- Configure network security controls, including firewalls and IDS/IPS.
- Set up authentication mechanisms and enforce MFA.
- Establish monitoring and logging capabilities.
- Conduct initial penetration testing and vulnerability assessments.

3. Post-Implementation Phase

- Perform final security validation through auditing and testing.
- Verify the effectiveness of logging, monitoring, and incident response mechanisms.
- Provide comprehensive documentation and handover procedures.
- Conduct security awareness training for stakeholders.
- Schedule periodic security reviews and updates.

These guidelines serve as a foundation for ensuring the security and reliability of MSSP systems managed by PT. NOOSC Security Global. By following structured security configurations and adhering to the inspection, implementation, and post-implementation checklist, NSG can maintain a high standard of security service delivery while ensuring compliance with industry best practices and regulations.

