**Threat hunting - using YARA signature to detect cyber attacks in the organization**

BS-CS-25-210

Shahar David; [shahardavid169@gmail.com](mailto:shahardavid169@gmail.com)  
Roi Zur; [tsurroi@gmail.com](mailto:tsurroi@gmail.com)

Advisor: Dr. Guy Tel-Zur

SCE - Shamoon College of Engineering, Be’er-Sheva

The challenge of detecting and mitigating malware threats transmitted via email is critical for maintaining the cybersecurity of organizational networks. This project develops an advanced information system that integrates email-specific YARA signatures with Suricata, an open-source network threat detection engine. Suricata monitors network traffic to identify real-time intrusions and supports various modes like intrusion detection system (IDS) and intrusion prevention system (IPS). It utilizes a comprehensive rule set for detecting complex threats such as malware and viruses, enhancing the capability to monitor, identify, and alert on malicious email activities efficiently. YARA rules are employed in this system to describe malware patterns, aiding in the automated detection and classification of malware across systems. These rules consist of strings and conditions, helping security teams quickly identify and respond to email-based threats. The integration of specialized YARA signatures for email with Suricata is designed to scan incoming email traffic effectively, providing immediate alerts on detected threats and enabling timely interventions to secure the network. Our approach involved rigorous testing with simulated email attack scenarios, aiming to optimize detection accuracy and reduce false positives. This system was developed based on an in-depth literature review of the latest advancements in email security and malware detection techniques, identifying key features needed to effectively counteract evolving email threats. The result is a dynamic system that significantly improves the network's security posture by offering real-time detection and alerts for email-based malware. It includes an easy-to-use interface for managing YARA rules, ensuring that the system remains current with the latest malware definitions and trends.

Keywords: malware detection; cybersecurity; YARA signatures; Suricata; network traffic analysis; IDS

**ציד איומים - שימוש בחתימות YARA לאיתור תקיפות סייבר בארגון**

BS-CS-25-210

שחר דוד; [shahardavid169@gmail.com](mailto:shahardavid169@gmail.com)  
רועי צור; [tsurroi@gmail.com](mailto:tsurroi@gmail.com)

בהנחיית: ד"ר גיא תל-צור

SCE - המכללה האקדמית להנדסה ע"ש סמי שמעון, באר שבע

האתגר של זיהוי ומניעת איומי תוכנות זדוניות שמועברות בדואר אלקטרוני חיוני לשמירה על אבטחת המידע ברשתות ארגוניות. פרויקט זה עוסק בפיתוח מערכת מידע מתקדמת שמשלבת חתימות YARA ספציפיות לדוא"ל עם Suricata, מנוע זיהוי איומים ברשת. Suricata מופעל במצבים כגון מערכת זיהוי חדירות (IDS) ומערכת מניעת חדירות (IPS), ומשתמש בסט כללים מקיף לזיהוי איומים כגון תוכנות זדוניות ווירוסים. השילוב של חתימות YARA לזיהוי דוא"ל עם Suricata מיועד לסרוק תנועת דוא"ל נכנסת ביעילות, ולהציע התראות מיידיות על איומים שזוהו.

המערכת פותחה לאחר סקירת ספרות על התקדמויות אחרונות באבטחת דוא"ל וזיהוי תוכנות זדוניות, ובדיקות רבות בתרחישי תקיפת דוא"ל דמויים לאימות דיוק הזיהוי והפחתת חיובים שגויים. התוצאה היא מערכת דינמית שמשפרת את מצב האבטחה של הרשת על ידי הצעת זיהוי והתראות בזמן אמת עבור תוכנות זדוניות בדוא"ל. המערכת תישאר מעודכנת עם הגדרות התוכנות הזדוניות והאיומים החדישים ביותר.

מילות מפתח: זיהוי תוכנות זדוניות; אבטחת סייבר; חתימות YARA; Suricata; ניתוח תעבורת רשת; מערכת זיהוי חדירות