FYP ABSTRACT 2024 SECURITY PROJECTS

Project # 2
Description:
The Wazuh and ELK stack has become a popular choice for organizations that require an open source, easy to use platform for log management and threat detection. This project proposes a system to detect anomalies using Artificial Intelligence (AI) algorithms in the open-source Wazuh/ ELK (Elastic Logstash Kibana) Security Suite. ELK provides a comprehensive analysis system for IT security, containing a centralized log server, a file integrity monitoring system, an intrusion detection system, and a Security Information and Event Management (SIEM) solution.

The proposed system will collect, analyze, and visualize data in ELK in real-time and apply use Machine Learning (ML) techniques to detect anomalies in logs. Specifically, it will utilize a range of AI algorithms to identify any deviation from the normal behaviour. Additionally, the system will alert the user in real-time when an anomalous event occurs with the threat level associated with the anomaly, followed by recommendations to mitigate the threat. Subsequently, Kibana will be used to visualize the data, allowing for easy exploration and further analysis.

Use cases:

1. Anomalous File Creation at Unusual Paths
2. Suspicious volume of logins to user account
3. Suspicious volume of logins to user account by logon Type
4. Anomalous SMB Connection by Device
5. Anomalous SMB Connection generated by File
6. Symbolic Link to Shadow Copy Created
7. Anormal Scheduled Task created
8. Abnormal Registry Changed
9. Anomalous Group Policy Changes
10. Unusual Remote Services Execution
11. Abnormal Large DNS Response
12. Unusual web browsing activity with Rare and Unusual URL
13. Abnormal traffic requesting the unusual endpoints
14. NAT Traversal Port Activity
15. Cobalt Strike Command and Control Beacon
16. Rare User Agents
17. Detect DNS tunnelling
18. Network Activity with Unusual domains
19. Anomalous Network Denies
20. Anomalous Network Activity

Key Skills: ELK, Wazuh, Machine Learning, Cyber Attacks