1. **MSc Project Proposal Form**

|  |  |
| --- | --- |
| **Student Number** | *Remove the italic red commentary and fill out all the fields* |
| **Student Name** |  |
| **Course Name** | *MSc …* |
| **Supervisor Name** |  |
| **Project Title** | SOC using advance techniques |
| **Description of your artefact** | There are several moving pieces in the construction of a Security Operations Center (SOC). From a technological standpoint, it is critical to rely on open source to identify hazards and decrease expenses. Many devices and technologies must be employed to develop the SOC from a DiD (Defense in Depth) perspective. Based on industry expertise, the technologies listed below can be utilised to create a proper SOC to monitor risks and discover anomalies in order to protect the firm.  Because the majority of assaults come from outside, it is critical to utilise adequate network perimeter controls. We may lower the cost of the product by employing open source products, and support is not required.  Aims:  This thesis aims to establish a secure virtual environment that allows Using built-in monitoring systems for safe adversary simulation and threat identification. Complex operations are feasible in this setting assaults or malware analysis, as well as testing the detection capabilities for adversary approaches, Providing SOCs with a greater understanding of current risks; improving detecting methods increase the SOC's capacity to defend organizations that are managed  Objective:  Despite the importance of threat in SOC, it is a time-consuming operation that requires personnel with experience to discover risks from millions of records. Threat-identifying teams at the enterprise level must go through each record in order. They must investigate each log, which must then be classed as harmful or non-malicious. By adding different tools to speed up the process, this work may be made easier. This research aims to employ tools to identify threats in SOC.  The artifact of this thesis are:   * The deployment must be reproducible using automation to enable various adversary emulation and detection evaluations. * This testing environment will be used to understand contemporary cyber threats better. * The execution of an attack using standard adversary methods and detection opportunities for these procedures. |
| **What methodology (structured process) will you be following to realise your artefact?** | We used multiple open source tools which available on github to identify threat in SOC. |
| **How does your project relate to your degree course and build upon the units/knowledge you have studied/acquired** | My MS degree is based on cyber security, so a SOC is an important component of a data security & data strategy since it helps limit information systems' vulnerability to external and internal dangers in the organization |
| **What are the main contributions of your project as compared to state-of-the-art?** | In this research, we highlight the problems of thinking like hackers, identifying exploitable flaws in technology, process, and people, or if we are too preoccupied with dealing with billions of logs pushed into SOC. This is the time to begin upgrading our SOC tools to automate and improve your organization's security posture.  Building and running a SOC presents some substantial hurdles. For one thing, upfront capital expenses might be exorbitant, which is not ideal for cash-strapped enterprises, even if the financial investment pays off in the long run with a decreased frequency of security disasters. Furthermore, external and internal security laws add complexity to the SOC creation process.  The issues, of course, do not cease once the SOC is fully functioning. Because SOCs concentrate security operations, SOC teams may use up to 20 distinct technology combinations; however, operational security management technology can provide a far more integrated feature set.  With the correct approaches, those frequent SOC issues may be overcome. To begin, corporations should not separate security strategy from their SOCs, which are primarily operational entities. Nonetheless, the objective of a SOC must be consistent with the organization's broader physical security plan. For starters, that plan will establish the organization's risk tolerance threshold. Furthermore, successful SOCs continue to grow to their organization's changing footprint.  Context-aware threat intelligence is critical in this case. And a SOC that does the initial threat assessment is considerably more likely to be effective than one that does not. That evaluation will assist staff in identifying physical security holes that require more attention (and protection), such as more granular understanding of layout and how employees function within their physical environment. |
| **Resources** | Tools:  Github: opensource software  Environment: Windows Operating System 64 Bit & Kali Linux  License: Openly licensed data and instruments  Hardware Equipment: The required computer resources, including routers and network server endpoints configured with Windows 7 and Windows 10.  University Resources, scholarly materials, and IEEE are reviewed  References:  Resul, D. A. (2020). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security Science 8.4* .  The Modern Security Operations Center, SecOps and SIEM: How They Work Together [online]. Exabeam [visited on 2021-05-05]. Available from: <https://www.exabeam.com/siem-guide/thesoc-secops-and-siem>  What are Indicators of Compromise (IoCs) Used For? [Online]. The MITRE Corporation, 2020 [visited on 2021-05-07]. Available from: https : / / lifars . com / 2020 / 05 / what - are - indicators - of - compromise-iocs-used-for  Shahjee, D. a. (2022). "Integrated Network and Security Operation Center: A Systematic Analysis (February 2022). *IEEE* .  Shmelkin, R. L. (2021). Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution. *In 2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021), pp. 01-08.*  Singh, P. a. (2021). Attack and intrusion detection in cloud computing using an ensemble learning approach. *International Journal of Information Technology 13, no.2* . |

1. **Project Plan and GANTT Chart**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Activity** | **Starting date** | **Target date** |
| 1 | Choose research area. |  |  |
| 2 | Literature search (find & confirm research gap). |  |  |
| 3 | Decide on research question and/or hypothesis. |  |  |
| 4 | Write the literature review draft. |  |  |
| 5 | Scope out research (initial thesis plan). |  |  |
| 6 | Write the proposal’s draft. |  |  |
| 7 | Submit the proposal. |  |  |
| 8 | Proposal approved. |  |  |
| 9 | Literature review. |  |  |
| 10 | Writing the report. |  |  |
| 11 | Submit the report 1 . |  |  |
| 12 | Feedback for report 1 |  |  |
| 13 | Submit report 2. |  |  |
| 14 | Feedback for report. |  |  |
| 15 | Submit entire report |  |  |
| 16 | Feedback the entire thesis. |  |  |