****

**School of Computing**

**Final Year Research Project**

**Project Initiation Document**

**Adam Cooper**

**Cyber Security and Forensic Computing**

**Artificially Intelligent SIEM for Targeted Threat Detection and Analysis**

# Basic details

|  |  |
| --- | --- |
| **Student Name** | Adam Cooper |
| **Draft Project Title** | Artificially Intelligent SIEM for Targeted Threat Detection and Analysis |
| **Course** | Cyber Security and Forensic Computing |
| **Project Supervisor** | Rahim Taheri |

# Degree suitability

This project dives into the application of an artificially intelligent Security Information and Event Management (SIEM) system. How artificial intelligence, more specifically machine learning, can be applied to a SIEM and will build on prior constructs from the Cyber Security and Forensic Computing course with the usage of Python, virtual machines, networking and identification of vulnerabilities through forensic investigation.

# The project environment and problem to be solved

The main audience of this project/report is cyber security analysts and those within security operation centres. These will be the main users of SIEM tools alongside threat detection and analysis tools that will be used daily to prevent attacks on the estate.

This research should provide a closer look into AI tooling for SIEM’s, specifically targeting threat detection and analysis to prevent noise, false positives and increase alerting infrastructure by providing a more in-depth alerting. Currently SIEM’s such as siembol and Apache Metron, which do not have any AI implemented, lack this and face the following issues:

* Alert Noise – Due to poorly setup or bad alerting.
* False positives – Poor alerting based on rules and not other activity.
* Alerts allowlisted not on a granular level – Activity excepted based on little common factors.
* Lack of consistency (i.e. alerts aren’t updated in time) – Rules have to be manually created and maintained.

Currently, AI in Cyber is still a niche sector with very few companies engaging in and implementing AI into their products. Similarly, and even more niche, AI used for threat detection and analysis with Artificially intelligent SIEM’s are only being provided by a handful of companies.

Some of the most recognisable being Elastic, Darktrace, Exabeam and Solarwinds.

Research Question:

Can AI effectively and accurately reduce alert noise from false positive alerting and similar previous activity whilst providing a more granular overview to alerting by implementing machine learning into a SIEM?

# Project aim and objectives

**Aim:** To successfully implement AI into a SIEM for increased efficiency of alerting and reducing alert noise

**Objectives:**

* Complete a review of previous works on AI SIEM implementations and machine learning for anomaly detection.
* Create virtual SOC environment to produce realistic results.
* Create Machine learning model.
* Train and test against previous datasets.
* Implement machine learning into SIEM to test against logs from SOC Environment
* Validate and Evaluation of results.
* Submit a project which has had an impact on the research aim and answered research questions.

# Project constraints

* Project timescale.
* Possibility of GDPR compliance issues.
* BCS code of conduct..
* University code of conduct
* Personal hardware limitations.

# Facilities and resources

Custom Desktop specification of:

* + Ryzen 5 3600 6-core (12 CPU)
  + AMD 5600XT 8GB
  + 48GB 3600
* Personal Laptop specification of:
  + I7 8700k
  + Quadro p2000
  + 32gb 2133
* VMware 17x – For creating the SOC Environment and collecting logs.
* VSCode – IDE for interacting with playbooks.
* Python 3.11x – Used for coding ML Algorithms.
* Microsoft 365 – Word processing software.
* Jira – Project Management.
* Supervisor – Mentoring & Advanced knowledge on subject.
* Google Scholar – Research Papers.
* IEEXplore – Research Papers.
* Internet – Research.

# Log of risks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Description** | **Likelihood**  **(high, medium, low)** | **Impact** | **Mitigation/Avoidance** |
|  | Data Loss | Medium | Delay to project will have to regather data | Once data is collected create a backup which is to be destroyed at the end of the project. |
|  | Total Hardware Failure | Low | Severe delays to project timeline and potentially impact performance – Loss of data and SOC Environment | Code backed up to Github private repository and work backed up to onedrive so this can be accessed elsewhere if needed |
|  | Laptop or Desktop Failure | Medium | Delay project and data loss | Create backups of work USB and external sources i.e. Onedrive/Github |
|  | Missed Deadline | Medium | Sets back project | Ensure deadlines are strictly kept to completing stages of project in advance |
|  | Corrupted Datasets | Low | Cause training data to become invalid or unusable | Create a backup of the superset dataset and backup trained sets. |
|  | Corrupted Virtual Machines | Low | Partial loss of SOC environment and logging/data ingest | Frequently take snapshots which will be backed up to both my laptop and desktop |
|  | Incorrect ML Algo | Medium | Setback project timeframe | Ensure algorithms used are correct for purpose |
|  | Inability to access internet | Medium | Unable to carry out research on machine learning algorithms, techniques or ingest data for logging a realistic scenario | I will have the option to use a backup connection should this problem occur. |

# Project deliverables

Artefacts which will be created as part of the project include a SOC environment to create a realistic attack scenario and provide as accurate as possible logs within the timeframe provided. Using a pre-made SIEM application I aim to ingest these logs and implement machine learning model trained on a superset of previous datasets aggregating both machine and network activity.

My report will include a variety of documentation including: previous works within the field, testing, system design, code along with future improvements and implementations.

# Project approach

Project management and delivery will use Agile and be maintained through Jira. Secondary research will be carried out in the form of a literature review covering machine learning for anomaly detection and artificially intelligent SIEMs. As the subject of AI is relatively new to me, I will also be learning this throughout the duration of the project by referencing official documentation.

In addition, I will also:

* Complete a review of machine learning models with what would be best suited for the project i.e., researching different algorithms for anomaly detection such as KNN and Decision trees.
* Build and develop a virtual environment, similar to a SOC for gathering attack data logs to simulate a real-life scenario for threat intelligence.
* Create machine learning model(s) and deploy against test data (aggregated datasets) and logs gathered from test environment.
* Implement system and model validation to confirm the model detected threats as expected and did not need altering.
* Evaluate both system and model to ensure they successfully fulfilled their requirements and explore potential improvements.

# Project Tasks and Timescales

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Stage** | **Dates** | **Main Tasks** |
|  | Project Start Up | 18/09/23 - 06/10/23 | Decide on project and find supervisor |
|  | PID | 06/10/23 – 20/10/23 | Complete PID |
|  | Build Linux Machines | 16/10823 – 20/10/23 | Create base virtual machines in VMWare 17 |
|  | Build windows Machines | 20/10/23 – 24/10/23 | Create base windows machines in VMWare 17 |
|  | Install T-POT | 25/10/23 – 26/10/23 | Install T-Pot on ubuntu server to act as a vulnerable access point within the network |
|  | Install SIEM | 26/10/23 – 29/10/23 | Install SIEM application which can have machine learning implemented |
|  | Aggregate Datasets | 29/10/23 – 03/11/23 | Aggregate multiple datasets to create a superset that can be used for training a machine learning model |
|  | Complete building SOC Environment | 20/10/23 – 20/11/23 | Complete building SOC environment – Finish implementation, testing etc. |
|  | Literature Review | 20/10/23 – 11/11/23 | Complete Secondary research – Have around 50-100+ articles of literature and research questions to build the project on |
|  | Build ML Models | 12/11/23 – 20/12/23 | Based on secondary research create machine learning model(s) |
|  | Train and Test models | 12/11/23 – 20/12/23 | Train and test machine learning model based on the superset of data |
|  | Implement model into SIEM | 12/11/23 – 20/12/23 | Implement these models into the SIEM to label incoming data |
|  | Gather logs to produce data | 21/12/23 – 12/01/24 | Open up network to conduct primary research gathering adversary attack data on the network. Carried out within a demilitarized zone (DMZ) |
|  | Dissertation Write-Up | 01/01/24 – 30/04/24 | Begin creating structure, formalising anything which has already been written, i.e., literature review and writing dissertation based on secondary and primary research |
|  | Continued Testing | 01/01/24 – 30/04/24 | Continue to test against logs or re-run against new log data which has been collected |
|  | Continued Research | 01/01/24 – 30/04/24 | Continue to research |
|  | Project submission | 01/04/24 – 30/04/23 | Finalise writeup during this month – Reading through ensuring everything makes sense and everything that is needed has been included:   * Graphs * Statistics * Citations * Appendices * …etc. |

# Supervisor Meetings

|  |  |  |
| --- | --- | --- |
| Timeframe | Description | Medium |
| Bi-Weekly | If anything, notable to be discussed or anything needs to be discussed regarding the project progression. | Email – In Person – Zoom |

# Legal, ethical, professional, social issues

Any work carried out within this project is my own work and tools that are used throughout will be opensource with their sources stated and compliance to their conducts along with GDPR to ensure that no personally identifiable (sensitive) information is being collected and/or processed, the university code of conduct and BCS code of conduct. Any data collected is to be destroyed at the end of the project.

There will be no human participants as part of this project, the network will be open to the public and therefore adversaries can engage and attack the network at their own will. The network will be separated from any other network, running in a demilitarized zone and all systems are run from within virtual machines.

There will be no financial inducements or risks to physical or environmental features, historical or cultural heritage. The project does not involve animals and will not be harmful to any third parties nor can it affect UK security.

**Appendix A: Gantt chart**

