**MAJOR PROJECT**

**SYNOPSIS**

**ON**

**SECURITY INFORMATION AND EVENT MANAGEMENT**

**Submitted By**

|  |  |  |  |
| --- | --- | --- | --- |
| BINEEK RAJA | VIKASH ANAND | MOHIT PANDEY | VANDANA SHARMA |
| 500037964 | 500037924 | 500040630 | 500041079 |
|  |  |  |  |

***Under the guidance of***

**Mr. JATIN SETHI**

Assistant Professor

Department of Computer Science & Engineering



**School of Computer Science and Engineering,**

**College of Engineering Studies,**

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**Dehradun-248007**

**2017**

****

**School of Computer Science and Engineering**

**University of Petroleum & Energy Studies, Dehradun**

**Project Proposal Approval Form (2017-18)**

**Major 1**

**Project Title: SECURITY INFORMATION AND EVENT MANAGEMENT**

***Abstract:***

**Security information and event management (SIEM)** technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources. There is a need to provide cost effective open source application that can provide threat detection through real time analysis of security alerts generated by network components which would be helpful for small organisations.

This application will provide real-time monitoring, correlation of events, notifications, console views and provides long-term storage as well as analysis, manipulation based on reporting of log data and security records.

**Introduction:**

Security information and event management (SIEM) software products and services combine [security information management](https://en.wikipedia.org/wiki/Security_information_management) (SIM) and [security event management](https://en.wikipedia.org/wiki/Security_event_manager)(SEM). They provide real-time analysis of security alerts generated by network hardware and applications.

The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is known as security event management (SEM). The second area provides long-term storage as well as analysis, manipulation and reporting of log data and security records of the type collated by SEM software, and is known as security information management (SIM).

The term security information event management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005,

* The product capabilities of gathering, analyzing and presenting information from network and security devices
* Identity and access-management applications
* [Vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) management and policy-compliance tools
* Operating-system, database and application logs
* External [threat](https://en.wikipedia.org/wiki/Threat_(computer)) data

A key focus is to monitor and help manage user and service privileges, [directory services](https://en.wikipedia.org/wiki/Directory_services) and other system-configuration changes; as well as providing log auditing and review and incident response.

Capabilities/Components:

* Data aggregation: [Log management](https://en.wikipedia.org/wiki/Log_management) aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
* Correlation: looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution[[7]](https://en.wikipedia.org/wiki/Security_information_and_event_management#cite_note-7)
* Alerting: the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.
* Dashboards: Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.[[8]](https://en.wikipedia.org/wiki/Security_information_and_event_management#cite_note-8)
* Retention: employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log [data retention](https://en.wikipedia.org/wiki/Data_retention) is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.

**Literature Review:**

SIEM or [Security Information and Event Management](http://wiki.aanval.com/wiki/Library:The_Essential_Features_and_Capabilities_of_a_SIEM_Technology) is defined as a complex set of technologies brought together to provide a holistic view into a technical infrastructure.The SIEM gives you a holistic, unified view into not only your infrastructure but also workflow, compliance and log management. A SIEM can provide a multitude of capabilities and services efficiently.

At its core, a SIEM provides:

* **Event and Log collection:** This may come in many forms, especially with in-house applications.
* **Layered Centric Views or Heterogeneous:** This is usually in the form of dashboards or “views,” referred to as a bird’s-eye view.
* **Normalization:** a two-part function. This includes translating computerized jargon to readable data to be displayed, and mapping data to user- or vendor-defined classifications/characterizations. This is sometimes referred to as “field mapping.”
* **Correlation:** This essentially gives the data context and forms relationships based on rules, architecture and alerts. This should be either historical or real-time.
* **Adaptability (Scalable):**This dumbs down to being able to speak the language regardless of source vendor, format, type, change or compliance requirement.
* **Reporting and Alerting:** This may be used to not only show value to executives but also provide automated verification of continuous monitoring, trends and auditing. Some would argue that the auditing aspect is an essential function but the SIEM alone does nothing – like a retired general with no troops or a SQL instance with no tables or data.
* **Log Management:** Allowing the capability for storing event and logs into a central location, while also allowing the application of compliance storage or retention requirements. (Again, many would argue this is a separate function, and I would disagree.)

**Problem Statement:**

* There is a need to provide cost effective open source application that can provide threat detection through real time analysis of security alerts generated by network components which would be helpful for small organisations.

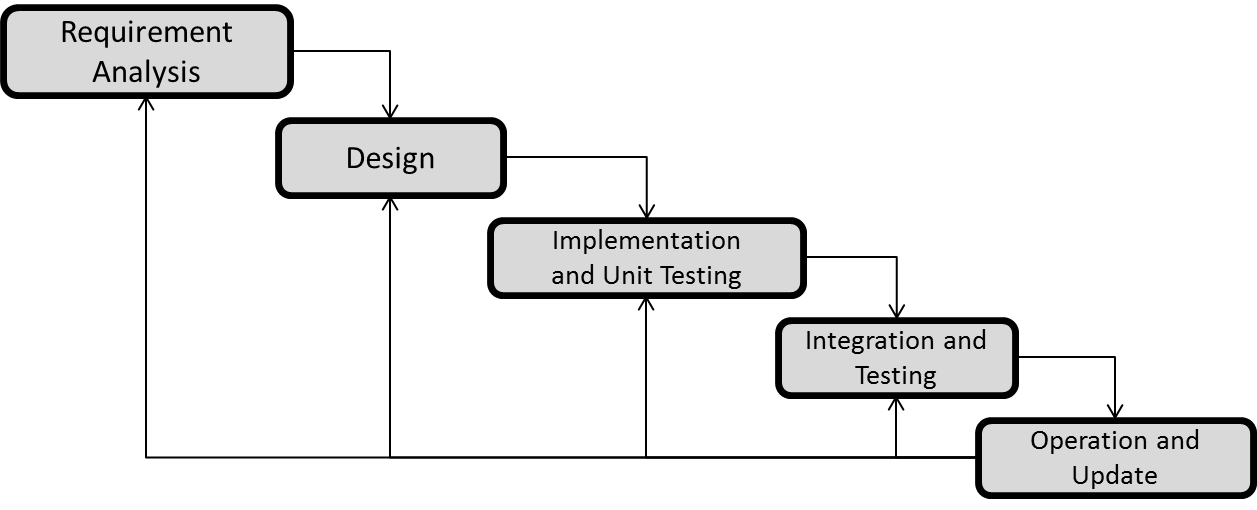
**Objectives:**

* To develop an application which can provide real-time monitoring, correlation of events, notifications, console views and provides long-term storage as well as analysis, manipulation and reporting of log data and security records.

**Methodology:**

We are using ITRERATIVE WATERFALL MODEL due to large data size and complexity of our project.

**ITERATIVE WATERFALL MODEL**

****

1. **Requirement Analysis:**

Data modelling i.e. collection of data which will be used as inputs and outputs.

1. **System Design:**An algorithm will be developed on the basis of formulas and data that are collected and will these data will be sampled as input in further phase. The algorithm will decrease the time complexity and will finally give an automated system for all the calculations under a single dashboard.
2. **Implementation and Unit Testing:**

We will develop the application using the algorithm developed during design phase in C language. The application will be developed in two modules and will be tested separately.

1. **Integration and Testing:**

The modules developed will be integrated to develop an application and tested by using the sample data collected during the analysis phase.

1. **Operation and Update:**

The final application developed will be deployed and updated according to the bugs which we will encounter.

**System Requirements:**

* **SOFTWARE REQUIREMENTS**

1. Language – Python 3
2. Compiler – Python
3. Operating System – Windows
4. IDE – PyCharm

* **HARDWARE REQUIREMENTS**
  1. 2 GHz dual core processor or better
  2. 2 GB system memory
  3. 25 GB of free hard drive space

**Schedule: (PERT Chart)**



**References:**

1. “*Successful SIEM and Log Management Strategies for Audit and Compliance*”

Swift, David, 4 November 2010

1. “*Magic Quadrant for Security Information and Event Management”*

Bussa, Toby & Kavanagh, Kelly, 10 August 2016

**Approved By**

**Mr. JATIN SETHI Dr. T P Singh**

**Project Guide Program Head**