SYNOPSIS

INDUSTRIAL TRAINING (TR-104)

SAFEAEON INC., MOHALI

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
Six Months of Industrial Training
at

(From 09/01/2023 to 09/05/2023)

SUBMITTED BY

NAME: ARSHDEEP SINGH
UNIVERSITY ROLL NO. 2004693

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GURU NANAK DEV ENGINEERING COLLEGE, GILL PARK, GILL ROAD, LUDHIANA

CONFIRMATION LETTER FROM THE COMPANY

SafeAeon Inc.
6701, Koll Center Parkway, Suite 250,
Pleasanton, California 94566, USA.

TO WHOM IT MAY CONCERN

This is to certify that Mr. Arshdeep Singh, S/O Mr. Harpreet Singh student of the Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Ludhiana, having Reg no- 2004693, has started an internship as a SOC Analyst from January 09, 2023, to till date under the guidance of the Senior team.

During his internship, he was exposed to different processes and was diligent, hardworking, and inquisitive.

We wish him a bright future.

Sincerely,

Date: June 01, 2023

Gurwinder Singh

Director of Talent Acquisition, SafeAeon Inc.

ABOUT THE COMPANY

Introduction to Organization

Founded in 2001, Wave strong is a U.S Silicon Valley based industry leader in providing Managed Cyber Security Operations Center (SOC) services for enterprise customers. At WaveStrong, we pride ourselves on our best of breed security solutions and services that span a myriad of government, education, and business verticals. To date, WaveStrong was providing all security services to its customers from its headquarters based out of Silicon Valley (Pleasanton, CA). SafeAeon is an effort to start a new venture and fix the gaping hole in WaveStrong business model of only using US resources for SOC service delivery.

SafeAeon's 24×7 Security Teams work around the clock to monitor, detect, and respond to cyber-attacks before they have the chance to impact your business. SafeAeon is your Armored Security Shield. Our highly trained, certified, and expert team providing exceptional services at an affordable price like never seen before. Enlist SafeAeon's security experts to help you achieve true digital resilience. Get the time advantage back so you can focus on your core competency.

Our Mission

Industry Leading Quality SOC at Industry beating prices for every business- Big or Small.

Our Vision

24/7 SOC Monitoring no longer fiefdom of privileged few.

Our Services

- Endpoint Detection and Response
- Database Audit and Monitoring
- Next-Gen Firewalls
- Patch Management
- Security Incident and Crisis Report
- Forensic Analysis
- Vulnerability Assessment
- Data Loss Prevention &Cloud Monitoring

OBJECTIVES OF THE TRAINING

Main Objectives of the training:

- Learn how QRadar SIEM collects the data to detect suspicious activities.
- Navigate and customize QRadar SIEM dashboard.
- Investigate vulnerabilities & services of assets.
- Create customized reports by tuning the QRadar.
- Make use of charts and apply filters to examine any specific activity in your env.
- Investigate policy breaches and suspected attacks.
- Search, filter, group and analyze security data.
- Locate custom rules and inspect actions & responses of rules.
- Alerts to suspicious activities and policy breaches in the environment.
- Provides deep visibility into network, user, application activity.
- Putting security relevant data form various sources in context of each other
- Provides reporting the templates to meet operational and compliance requirements.

HARDWARE & SOFTWARE TO BE USED

Technical Requirements for QRadar SIEM:

To successfully deploy and operate QRadar SIEM, it is important to consider both the software and hardware infrastructure requirements. Here are the key technical requirements for QRadar SIEM:

1. **Hardware Requirements:**

a. **Server Hardware:** QRadar SIEM requires a dedicated server infrastructure to host the SIEM solution. The server should meet the recommended specifications in terms of processing power, memory, and storage capacity to ensure optimal performance and scalability.

b. **Network Infrastructure:** A robust and reliable network infrastructure is essential for QRadar SIEM deployment. This includes network switches, routers, and firewalls that can handle the traffic generated by the SIEM solution. Adequate bandwidth and network connectivity are crucial for seamless data collection and transmission.

2. **Software Requirements:**

a. **Operating System:** QRadar SIEM is designed to run on Red Hat Enterprise Linux (RHEL) Server. It is important to ensure that the server meets the version and compatibility requirements specified by QRadar SIEM for RHEL.

b. Java SDK: QRadar SIEM relies on the IBM Runtime Environment Java Technology edition 7.0.8. It is necessary to install and configure the required Java Development Kit (JDK) to ensure proper functioning of the SIEM solution.

c. **Security Management:** Tivoli Directory Integrator 7.1.7 is a critical component for effective security management in QRadar SIEM. This software helps integrate directory services, enabling user authentication and authorization within the SIEM environment.

3. **Browser Requirements:** To access and utilize the QRadar SIEM user interface, specific browser versions and future fix packs are recommended. The following browsers are supported:

a. **Google Chrome:** QRadar SIEM supports Google Chrome version 43 and future fix packs, ensuring compatibility and optimal performance when accessing the SIEM interface.

b. **Microsoft Internet Explorer:** QRadar SIEM is compatible with Microsoft Internet Explorer version 10 and future fix packs. It is important to use the recommended browser version to ensure a seamless user experience and access to essential security features.

c. **Mozilla Firefox ESR:** QRadar SIEM supports Mozilla Firefox Extended Support Release (ESR) version 38 and future fix packs. Utilizing this specific version of Firefox ESR guarantees compatibility and a stable browsing environment for QRadar SIEM.

By meeting these hardware and software requirements, organizations can ensure the successful deployment and operation of QRadar SIEM. It is essential to have the necessary server infrastructure, network components, and compatible software to enable efficient security monitoring, threat detection, and incident response within the SIEM environment.

WHAT CONTRIBUTION WOULD THE TRAINING MAKE?

a. In my role at SafeAeon, I will contribute significantly to the implementation and utilization of IBM QRadar as our chosen SIEM solution. I will play a crucial part in ensuring the optimal protection of our clients' businesses by leveraging the exceptional features and capabilities of IBM QRadar.

b. One of my key contributions will involve tailoring the deployment of IBM QRadar to meet the specific requirements of each client's organization. I will work closely with the Security Teams to determine whether a hardware, software, or virtual appliance-based deployment is most suitable. This flexibility will allow us to seamlessly integrate the SIEM solution into the existing infrastructure of our clients, regardless of its scale or complexity.

c. Furthermore, I will actively contribute to enhancing the efficiency and effectiveness of our Security Operations Center (SOC) analysts. I will collaborate with the team to maximize the benefits of IBM QRadar's architecture, ensuring that event processors effectively collect, store, and analyze event data while event collectors efficiently capture and forward data. By optimizing this comprehensive approach, I will enable our analysts to have a holistic view of our clients' networks, enabling swift and accurate threat detection.

d. As part of the SOC team, I will work closely with SOC analysts, providing them with support and expertise in utilizing the various capabilities of IBM QRadar. This includes effectively utilizing flow processors to capture layer 4 network flows, leveraging QFlow processors for deep packet inspection of Layer 7 application traffic, and utilizing centralized consoles for streamlined management. By actively contributing to the integration of these features, I will empower our SOC analysts with comprehensive visibility into our clients' network environments, ensuring that potential threats are identified and addressed promptly.

e. Additionally, I will assist in managing the SIEM infrastructure, particularly the integrated appliance model offered by IBM QRadar. By ensuring the smooth operation of the console and event/flow processors, I will enable our SOC analysts to focus on their core responsibilities of monitoring and responding to security incidents. Moreover, I will explore the possibilities of utilizing IBM QRadar as a SAAS offering on the IBM cloud, which will allow for seamless deployment and maintenance, further enhancing the efficiency and effectiveness of our security solution.

f. Through my active involvement in leveraging the advanced capabilities of IBM QRadar, I will play a vital role in establishing robust and proactive security measures for our clients' businesses at SafeAeon. By ensuring that our SOC analysts have access to cutting-edge tools, I will contribute to their ability to protect our clients' organizations effectively against emerging cyber threats.

THE SCHEDULE OF THE TRAINING

The training program I will be undertaking spans a comprehensive duration of six months, commencing on January 9, 2023, and concluding on July 8, 2023. Throughout this extended period, I will immerse myself in intensive learning and skill-building activities. To ensure maximum engagement and progress, I will dedicate myself to the training five days a week, from Monday to Friday.

ROLE AT THE TRAINING SITE

During the first six months of my tenure as a SOC analyst intern, I will play a vital role in the company's security operations center. My primary responsibilities will involve working with advanced tools and technologies such as SIEM (Security Information and Event Management) and EDR (Endpoint Detection and Response) systems. I will be trained on various SIEM platforms, including IBM QRadar, Splunk, Elastic, and Microsoft Sentinel, enabling me to effectively monitor and analyze security events and incidents.

In the coming months, I will become proficient in using SIEM consoles to monitor and investigate alerts generated by these platforms. I will work closely with senior analysts to understand the incident response process, learning how to triage and prioritize security events for efficient resolution. Additionally, I will have the opportunity to gain hands-on experience with EDR solutions like CrowdStrike Falcon, Carbon Black, or SentinelOne. This will involve deploying and managing EDR agents on endpoints, analyzing alerts, and actively participating in incident response activities.

As an intern, I will collaborate closely with the experienced SOC analysts, contributing to the development of security playbooks and participating in simulated incident response exercises. These activities will allow me to enhance my understanding of common attack vectors and techniques, while also strengthening my skills in incident detection, analysis, and response. Throughout my internship, I aim to contribute to the organization's overall security posture and gain practical knowledge that will be invaluable as I progress in my career in cybersecurity.

In summary, as a SOC analyst intern during the first six months of my tenure, I will immerse myself in the world of cybersecurity, working with SIEM and EDR systems such as QRadar, Splunk, Elastic, and SentinelOne. I will actively monitor and investigate security events, participate in incident response activities, and collaborate with experienced analysts. This internship will provide me with the necessary skills and knowledge to excel in the field of cybersecurity and make valuable contributions to the company's security operations.