**WEEK 6 ASSIGNMENT**

1. What is SIEM and what are some of the importance of having SIEM in your network?
2. Name some vendors with SIEM
3. What some of the role of SIEM for businesses?
4. What does SIEM stand for?

A) Security Information and Event Monitoring

B) Security Information and Event Management

C) Security Incident and Event Management

D) Security Incident and Event Monitoring

1. Name some of the Protocols for network centric?
2. What are some capabilities of SIEM?
3. Which of the following is NOT a primary function of a SIEM system?

A) Collecting security-related data from various sources

B) Correlating and analyzing security-related events

C) Providing intrusion detection and prevention capabilities

D) Performing vulnerability assessments

1. Which of the following is NOT a typical data source for a SIEM system?

A) Network devices (routers, switches, firewalls)

B) Servers (Windows, Linux, Unix)

C) Databases (Oracle, SQL Server)

D) Social media platforms (Facebook, Twitter)

1. What is the purpose of correlation rules in a SIEM system?

A) To detect security incidents by correlating related events from different sources

B) To determine the root cause of security incidents

C) To identify vulnerabilities in the network

D) To generate reports on security-related activities

1. What is the benefit of using a SIEM system for threat detection and response?

A) Faster incident response times

B) Improved accuracy of threat detection

C) Reduced false positive alerts

D) All of the above

1. What are some capabilities of SIEM?