1. Project Initialization

1.1 Planning and Design

1.1.1 Analyze the existing infrastructure, systems, and security controls

Analyzing the existing infrastructure, systems, and security controls for cyber security requires a comprehensive assessment of various components to ensure the protection of sensitive data and prevent unauthorized access.

Infrastructure Assessment:

- Network Architecture
- Cloud Environment
- Physical Security

System Assessment:

- Operating Systems
- Endpoint Security
- Security Controls Assessment
  a). Access control
  b). Encryption
  c). Intrusion Detection and Prevention
  d). Firewalls
  e). Security Information and Event Management (SIEM)

Security Policies and Procedures:

- Incident Response Plan
- Data Handling and Classification
- Employee Training

Compliance and Regulatory Considerations:

- Industry Standards
- Regulatory Compliance

Risk Assessment:

- Vulnerability Management
- Thread Landscape

1.1.2 Architecture and Deployment for QRadar SOC/SIEM:

Components and Layers:

- Data Sources
- Event Collectors
- Event Processor
- Flow Processors
- Data Store

- SIEM Console
- Analytics Engine
- Incident Response
- Reporting and Dashboards
- Integration Hub

Deployment Strategy:

- Sizing and Scalability
- High Availability
- Geographical Distribution
- Virtualization
- Data Retention
- Data Collection Strategy
- Security controls
- Regular Maintenance
- User Training
- Integration with Existing Infrastructure
- Testing and Tuning

The QRadar SOC/SIEM implementation is an iterative process. It's important to continually review and refine the architecture and deployment strategy based on changing organizational needs and the evolving threat landscape. Additionally, involving cyber security experts or consultants with experience in QRadar can greatly enhance the effectiveness of the implementation.

1.1.3 Develop use cases, rules, and correlation logic based on security requirements

Developing use cases, rules, and correlation logic for a SIEM system like QRadar is a critical step to effectively detect and respond to security threats. Here are examples of use cases along with corresponding rules and correlation logic based on various security requirements:

Use case: Unauthorized Access Detection

Rule 1: Failed Logins

Correlation Logic: Account Lockouts Followed by Successful Login

Use Case: Malware Activity Detection

Rule 2: Suspicious Outbound Traffic

Correlation Logic: Multiple Anomalies in a short time

Use Case: Data Exfiltraion Detection

Rule 3: Large Data Transfer to External IP

Correlation Logic: Unusual Data Transfer and User Account Activity

1.1.4 Create a project plan with timelines, resource allocation and dependencies

Creating a comprehensive project plan involves breaking down the implementation of the QRadar SOC/SIEM system into manageable tasks, assigning resources, estimating timelines, and identifying dependencies. Here is a simplified project plan template.