Software Assurance: CSS321

A Pet Nose Best: Comprehensive Software Assurance Guidelines

Antoine Gaton

October 6, 2024

Table of Contents

**Project Outline3**

**Security in the Development Life Cycle4**

**Software Assurance Techniques6**

Analysis of Software Applications**6**

Guidelines for Software Assurance Techniques**8**

**Security in Nontraditional Development Models10**

Major Steps and Potential Security Threats**10**

Policies and Processes to Minimize Security Threats**11**

**Security Static Analysis15**

Component Diagram**15**

Code Sample**16**

Guidelines for Using Static Analysis Tools**19**

**Software Assurance Policies and Processes21**

Software Developer Training Plan**21**

Software Assurance Metrics**22**

**Security Team Roles and Responsibilities23**

# Project Outline

1. Organization
   1. *A Pet Nose Best*
      1. This organization provides both desktop and web-based software solutions for pet care service management, focusing on both private-sector pet care companies and government contracts related to pet licensing and animal welfare.
         1. *Note: This is my fiancé’s business which I am using as inspiration for this individual project.*
   2. Company Size
      1. Medium-sized: Approximately 150 employees
   3. Locations
      1. Miami
      2. New York
      3. San Francisco
      4. Austin
   4. Application
      1. Pet Care Management System (PCMS)
         1. Desktop application
      2. Government Pet Licensing Portal
         1. Web/Mobile application
   5. Database
      1. SQL Server
         1. Used for the PCMS desktop application.
      2. Firebase
         1. Used for the government per licensing portal.
2. Software Development Organization
   1. The software development team includes developers, QA engineers, DevOps, and security engineers, all reporting through the CTO. The company follows standard software development practices, including using Git for source control, CI/CD pipelines with Jenkins, and Jira for project management.

# Security in the Development Life Cycle

1. **Using Agile Methodology**
   1. **Sprint Planning**
      1. **Security Component**: Incorporate security requirements as part of the user stories. This includes prioritizing security tasks and defining security acceptance criteria for each sprint.
      2. **Tasks**: Conduct a threat model, identify potential risks, and ensure security requirements are added to the product backlog.
   2. **Design and Architecture in Sprint**
      1. **Security Component**: Continuous security architecture review. With each new feature or update, the design is evaluated for security risks.
      2. **Tasks**: Perform lightweight design reviews with a focus on security in each sprint and ensure any new security implications are documented.
   3. **Development (Coding) in Sprint**
      1. **Security Component**: Secure coding practices are integrated into each sprint. Developers adhere to secure coding standards and follow best practices for preventing security vulnerabilities.
      2. **Tasks**: Conduct peer reviews and code analysis focused on security vulnerabilities during the development process.
   4. **Testing (Quality Assurance) in Sprint**
      1. **Security Component**: Continuous security testing. Both manual and automated tests are conducted to identify potential security vulnerabilities.
      2. **Tasks**: Perform ongoing security testing, such as static analysis, dynamic testing, and penetration testing, as part of the sprint's quality assurance activities.
   5. **Sprint Review and Retrospective**
      1. **Security Component**: Evaluate security outcomes from the sprint. Identify what security issues were addressed and what vulnerabilities remain.
      2. **Tasks**: Review the security acceptance criteria and discuss any security concerns that arose during the sprint. Update the backlog with any new security tasks or issues.
   6. **Ongoing Monitoring and Maintenance**
      1. **Security Component**: Post-release, continuously monitor for security incidents. Security is not a one-time effort but rather a constant process of patching and updating.
      2. **Tasks**: Implement security patches, monitor for vulnerabilities, and respond to incidents in real-time. Conduct regular security reviews even after product deployment.

# Software Assurance Techniques

**Analysis of Software Applications**

**1. Pet Care Management System (PCMS) - Desktop Application**

* **Description**: The PCMS is a desktop-based software application designed for private pet care companies. It allows for managing client and pet data, appointments, services, and invoicing. The application stores sensitive data in a local SQL Server database.
* **Security Risks:**
  + **User Authentication and Authorization**
    - ***Threat***: Unauthorized access to client and pet data due to weak authentication mechanisms.
    - ***Implications***: Compromised sensitive data, legal liabilities, and loss of client trust.
    - ***Mitigation***: Implement multi-factor authentication (MFA) and role-based access control (RBAC). Using MFA ensures that even if login credentials are stolen, an additional layer of verification prevents unauthorized access. RBAC limits users to only the information and actions necessary for their role.
  + **Database Security**:
    - ***Threat***: SQL injection attacks that exploit vulnerabilities in the application’s database queries.
    - ***Implications***: Data breaches, data loss, and potential financial losses.
    - ***Mitigation***: Employ parameterized queries or stored procedures to prevent SQL injection. Regular vulnerability scans should also be conducted to ensure that the application is not susceptible to this attack.

**2. Government Pet Licensing Portal - Web/Mobile Application**

* **Description**: This web-based application serves as a portal for local governments to manage pet licensing and related information. It is accessible through both browsers and mobile devices, using Firebase for data storage.
* **Security Risks**:
  + **Cross-Site Scripting (XSS)**
    - ***Threat***: Malicious scripts injected into the website, compromising user data and sessions.
    - ***Implications***: Loss of sensitive government data, user accounts being hijacked, and exposure to future attacks.
    - ***Mitigation***: Implement content security policies (CSP) and sanitize all input fields. CSP prevents unauthorized scripts from running, while input sanitization ensures user inputs are safely processed.
  + **Data Transmission Security**:
    - ***Threat***: Man-in-the-middle attacks during data transmission, leading to the interception of sensitive information such as pet registration and user credentials.
    - ***Implications***: Breaches in the confidentiality of government information, data leaks, and public distrust.
    - ***Mitigation***: Ensure all data transmission uses secure communication protocols like HTTPS with Transport Layer Security (TLS). Also, enforce the use of strong encryption methods to protect data in transit.

**3. Pet Tracking Mobile App**

* **Description**: A mobile application that allows users to track their pets using GPS. The app store’s location data and user preferences in the cloud, likely integrating with Firebase for cloud services.
* **Security Risks**:
  + **Location Data Leakage**
    - ***Threat***: Unauthorized access to real-time GPS data, allowing tracking of users and pets.
    - ***Implications***: Physical safety risks for users and pets, breaches of privacy laws, and reputational damage.
    - ***Mitigation***: Implement strong encryption for stored and transmitted location data. Use anonymization techniques to protect users' identities when sharing location information.
  + **Mobile Device Security**
    - ***Threat***: Compromised mobile devices accessing the app, exposing sensitive data and user accounts.
    - ***Implications***: Data breaches, unauthorized control over the app, and exposure to malware.
    - ***Mitigation***: Use device-specific encryption and enforce biometric authentication (e.g., fingerprint or facial recognition). Additionally, regular updates should patch any discovered vulnerabilities in mobile platforms.

**Guidelines for Software Assurance Techniques**

1. **Desktop Applications**

* **User Authentication and Authorization**:
  + Implement Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC).
  + Secure login mechanisms, including password complexity requirements and lockout policies after repeated failed login attempts.
  + Regularly review and audit access control logs to detect any unauthorized attempts.
* **Database Security**:
  + Use parameterized queries or stored procedures to protect against SQL injection attacks.
  + Conduct regular database vulnerability assessments and implement real-time monitoring for suspicious activities.
  + Apply database encryption techniques for sensitive data storage.

1. **Web Applications**

* **Cross-Site Scripting (XSS) Prevention**:
  + Sanitize all user inputs using whitelisting approaches, and escape output to prevent malicious code execution.
  + Implement Content Security Policy (CSP) to limit the execution of unauthorized scripts.
  + Regularly perform dynamic and static code analysis to detect XSS vulnerabilities early.
* **Data Transmission Security**:
  + All data between the client and the server should be transmitted using TLS with strong encryption ciphers.
  + Implement HTTP Strict Transport Security (HSTS) to ensure that the application can only be accessed over secure connections.
  + Use encryption for sensitive data stored in the cloud (e.g., government licensing data).

1. **Mobile Applications**

* **Location Data Protection**:
  + Encrypt GPS and personal information both at rest and during transmission to cloud services.
  + Use anonymization for location data before sharing or storing it to avoid exposing users' exact locations.
* **Mobile Device Security**:
  + Enforce strong device authentication methods, such as biometric authentication or device-specific encryption.
  + Ensure that the mobile app is frequently updated to patch known vulnerabilities.
  + Use secure APIs to communicate between mobile apps and cloud services.

# Security in Nontraditional Development Models

**Non-Traditional Development Model: DevSecOps**

For A Pet Nose Best, I recommend implementing a DevSecOps model. This non-traditional approach integrates security practices within the DevOps process, ensuring that security is a shared responsibility throughout the entire software development lifecycle.

**Major Steps and Potential Security Threats**

**1. Plan**

**Description**: In this phase, project requirements are gathered, and the development strategy is outlined.

**Potential Security Threats**:

* Inadequate security requirements specification
* Overlooking potential security risks in the planning stage

**2. Code**

**Description**: Developers write code for the application features.

**Potential Security Threats**:

* Introduction of security vulnerabilities through insecure coding practices
* Use of outdated or vulnerable third-party libraries

**3. Build**

**Description**: The application is compiled and built into an executable form.

**Potential Security Threats**:

* Inclusion of sensitive information (e.g., API keys, passwords) in the build artifacts
* Use of insecure build tools or processes

**4. Test**

**Description**: The application undergoes various testing phases, including unit testing, integration testing, and user acceptance testing.

**Potential Security Threats**:

* Insufficient security testing coverage
* Failure to identify critical security vulnerabilities

**5. Release**

**Description**: The application is prepared for deployment to production environments.

**Potential Security Threats**:

* Unauthorized changes to release artifacts
* Insecure handling of production credentials

**6. Deploy**

**Description**: The application is deployed to production environments.

**Potential Security Threats**:

* Misconfiguration of production environments
* Exposure of sensitive data during deployment

**7. Operate**

**Description**: The application runs in production, serving end-users.

**Potential Security Threats**:

* Runtime vulnerabilities
* Inadequate monitoring for security incidents

**8. Monitor**

**Description**: The application and infrastructure are continuously monitored for performance and security issues.

**Potential Security Threats**:

* Delayed detection of security breaches
* Insufficient logging of security-relevant events

**Policies and Processes to Minimize Security Threats**

**1. Plan**

**Policy**: Security Requirements Integration

* All project plans must include explicit security requirements.
* Threat modeling must be conducted for each new feature or major change.

**Process**:

1. Include a security expert in all planning meetings.
2. Use a standardized security requirements checklist for each project.
3. Conduct and document threat modeling sessions for each new feature.

**2. Code**

**Policy**: Secure Coding Standards

* All developers must adhere to the company's secure coding guidelines.
* Regular code reviews with a focus on security must be conducted.

**Process**:

1. Implement automated code analysis tools in the development environment.
2. Conduct peer code reviews with a security checklist before any merge.
3. Maintain an up-to-date inventory of approved and vetted third-party libraries.

**3. Build**

**Policy**: Secure Build Process

* All build processes must be automated and version-controlled.
* Sensitive information must never be hard-coded in the source.

**Process**:

1. Use a secure, centralized secret management system for handling sensitive data.
2. Implement automated checks to detect hard-coded secrets in the codebase.
3. Ensure all build tools are regularly updated and securely configured.

**4. Test**

**Policy**: Comprehensive Security Testing

* Automated security testing must be integrated into the CI/CD pipeline.
* Penetration testing must be conducted before major releases.

**Process**:

1. Integrate SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) tools into the CI/CD pipeline.
2. Conduct regular security-focused test scenarios as part of QA processes.
3. Engage third-party penetration testers for annual security assessments.

**5. Release**

**Policy**: Secure Release Management

* All releases must go through a security sign-off process.
* Release artifacts must be cryptographically signed.

**Process**:

1. Implement a release checklist that includes security verification steps.
2. Use a secure, audited process for managing and rotating production credentials.
3. Implement artifact signing in the release process and verify signatures before deployment.

**6. Deploy**

**Policy**: Secure Deployment Practices

* All production deployments must use infrastructure-as-code principles.
* Deployment processes must be fully automated with minimal human intervention.

**Process**:

1. Use version-controlled infrastructure-as-code tools (e.g., Terraform) for all deployments.
2. Implement automated configuration checks post-deployment to verify security settings.
3. Use blue-green deployment strategies to minimize risk and enable quick rollbacks.

**7. Operate**

**Policy**: Runtime Security Monitoring

* All production systems must have real-time security monitoring enabled.
* Incident response plans must be in place and regularly tested.

**Process**:

1. Implement a SIEM (Security Information and Event Management) system for centralized logging and alerting.
2. Conduct regular security drills to test incident response procedures.
3. Implement runtime application self-protection (RASP) tools where applicable.

**8. Monitor**

**Policy**: Proactive Security Monitoring and Response

* Security-relevant events must be logged and retained for at least one year.
* Regular security reports must be generated and reviewed by the security team.

**Process**:

1. Implement automated alerting for suspicious activities or potential security breaches.
2. Conduct weekly security review meetings to discuss monitoring reports and address any concerns.
3. Regularly update monitoring rules and alert thresholds based on emerging threats and past incidents.

# Security Static Analysis

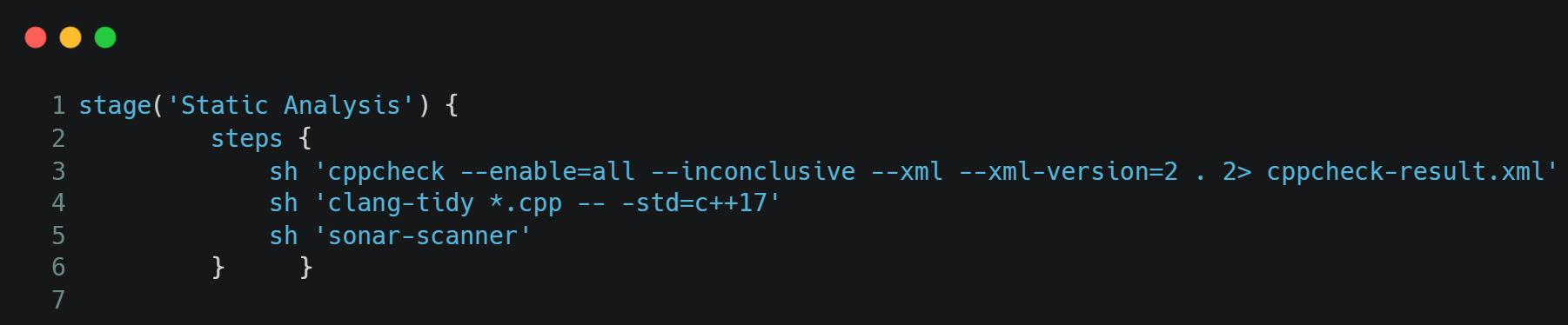
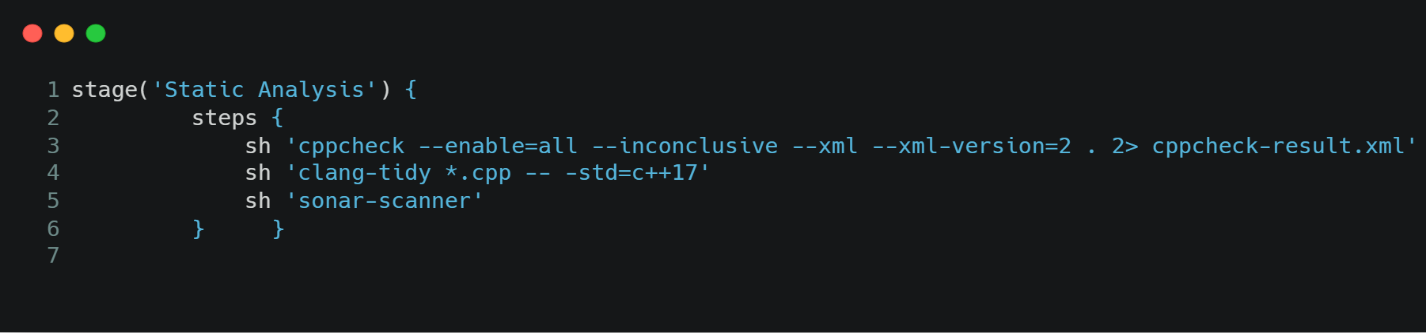
* Application Design: Pet Tracking System
  + *A Pet Nose Best* is developing a Pet Tracking System, a C++ application that allows pet owners to monitor their pets' location and activities in real-time. This system integrates with GPS-enabled collars and provides a user interface for pet owners to view their pets' location, set up geofences, and receive alerts.
* **Major Components**
  + *GPS Data Receiver*: Interfaces with pet collars to receive location data.
  + *Data Processing Module*: Processes and stores location data.
  + *User Interface*: Allows users to view pet locations and manage settings.
  + *Alert System*: Generates and sends notifications to users.
  + *Database*: Stores user accounts, pet information, and location history.
* **Component Diagram**

A diagram of a system

Description automatically generated

* **Potential Security**
  + *GPS Data Receiver*:
    - Potential for malicious data injection
    - Unauthorized access to raw location data
  + *Data Processing Module*:
    - Buffer overflow vulnerabilities
    - Insecure data handling
  + *User Interface*:
    - Cross-site scripting (XSS) in web interface
    - Insecure authentication mechanisms
  + *Alert System*:
    - Potential for sending alerts to unauthorized recipients
    - Denial of service through alert flooding
  + *Database*:
    - SQL injection vulnerabilities
    - Inadequate access controls
* **Code Samples**
  + A screen shot of a computer program

    Description automatically generatedSecure Input Validation (GPS Data Receiver)
  + A screen shot of a computer code

    Description automatically generatedSecure Data Storage (Database Interface)
  + Secure Alert System
* **Security Static Analysis Tools**
  + *Cppcheck*
    - Open-source static analysis tool for C/C++ code
    - Detects various types of bugs, including buffer overflows and memory leaks.
  + *Clang Static Analyzer*
    - Part of the Clang/LLVM project
    - Finds bugs in C, C++, and Objective-C programs
  + *SonarQube*
    - Multi-language static code analysis tool
    - Provides a wide range of code quality and security metrics
* **Guidelines for Using Static Analysis Tools**
  + *Integration into CI/CD Pipeline*:
    - Integrate these tools into the continuous integration/continuous deployment (CI/CD) pipeline to automatically analyze code with each commit or pull request.
      * Example: Jenkins using Groovy to add a stage for static analysis:
  + *Regular Scans*:
    - Schedule weekly full codebase scans using these tools to catch any issues that might have been missed in incremental scans.
  + *Custom Rule Sets*:
    - Develop and maintain custom rule sets for each tool that align with Industry and *A Pet Nose Best*'s coding standards and security requirements.
      * Example: Create `.clang-tidy` file in the project root using YAML:
  + *Severity-based Issue Handling*:
    - Categorize issues by severity and set appropriate response times:
      * Critical: Must be fixed immediately before merging
      * High: Must be fixed within 24 hours
      * Medium: Must be addressed within one week
      * Low: Should be addressed in the next two weeks
  + *False Positive Management*:
    - Maintain a list of confirmed false positives to prevent recurring noise in scan results.
    - Regularly review and update this list to ensure it remains accurate.
  + *Developer Training*:
    - Conduct quarterly training sessions on common issues detected by these tools and how to fix them.
    - Encourage developers to run these tools locally before pushing code.
  + *Compliance Reporting*:
    - Generate monthly reports from these tools to track progress in code quality and security.
    - Use these reports in compliance audits and security reviews.
  + *Tool-specific Guidelines*:
    - Cppcheck:
      * Run with all checks enabled: `cppcheck --enable=all --inconclusive`
      * Use the `--xml` flag to generate reports that can be easily parsed and integrated into other tools.
    - Clang Static Analyzer:
      * Use scan-build with your build system: `scan-build make`
      * Focus on the checker groups most relevant to security, such as `alpha.security.\*` and `security.\*`
    - SonarQube:
      * Set up quality gates in SonarQube to prevent merging of code that doesn't meet certain quality criteria.
      * Use SonarLint in developers' IDEs to catch issues before they reach the shared repository.

# Software Assurance Policies and Processes

* **Software Developer Training Plan**
  + To ensure that all software developers at A Pet Nose Best are well-versed in the new software assurance guidelines, we will implement the following training plan:
    - *Initial Comprehensive Training*
      * Duration: 2-day workshop
      * Format: In-person or virtual, depending on location
      * Content:
        + Introduction to software assurance concepts
        + Detailed walkthrough of A Pet Nose Best's software assurance guidelines
        + Hands-on exercises applying security practices to real-world scenarios
        + Introduction to static analysis tools

Cppcheck

Clang Static Analyzer

SonarQube

* + - *Monthly Security Brown Bag Sessions*
      * Duration: 1-hour lunch and learn sessions
      * Format: Virtual, company-wide
      * Content:
        + Updates on emerging security threats
        + Best practices spotlight
        + Q&A session with security team
    - *Quarterly Secure Coding Workshops*
      * Duration: Half-day workshop
      * Format: In-person or virtual, by development team
      * Content:
        + Deep dive into specific security topics (e.g., input validation, authentication mechanisms)
        + Code review exercises
        + Tool-specific training (rotating focus on Cppcheck, Clang Static Analyzer, SonarQube)
    - *Annual Security Certification*
      * All developers must complete an internal security certification annually
      * Online course with final assessment
      * Covers all aspects of A Pet Nose Best's software assurance guidelines
    - *New Hire Onboarding*
      * Dedicated 1-day security training as part of new hire onboarding
      * Covers basics of software assurance and company-specific guidelines
      * Assigned security mentor for first three months
    - *Continuous Learning Platform*
      * Access to online learning platforms (e.g., Pluralsight, Udemy) with curated security courses
      * Gamified learning system with rewards for completing security-related courses and challenges
* **Software Assurance Metrics**
  + To track the effectiveness of our software assurance efforts, we will collect and analyze the following metrics:
    - *Vulnerability Density*
      * Description: Number of vulnerabilities per 1000 lines of code
      * Collection Method: Automated through static analysis tools during CI/CD pipeline
      * Usage: Track trends over time; target continuous reduction
    - *Time to Fix Security Issues*
      * Description: Average time taken to address identified security vulnerabilities
      * Collection Method: Jira tickets tagged with security labels
      * Usage: Ensure timely resolution of security issues; identify areas needing more resources
    - *Security Debt*
      * Description: Total estimated time required to address all known security issues
      * Collection Method: Aggregated from Jira tickets and static analysis reports
      * Usage: Prioritize security work; justify resources for security initiatives
    - *Security Training Completion Rate*
      * Description: Percentage of developers who have completed required security training
      * Collection Method: Learning Management System (LMS) reports
      * Usage: Ensure all team members are up to date on security practices
    - *Security Review Pass Rate*
      * Description: Percentage of code changes that pass security review on first submission
      * Collection Method: Code review tool (e.g., Gerrit) with security review checkbox
      * Usage: Measure effectiveness of developer security practices and training
    - *Number of Security Incidents*
      * Description: Count of security breaches or near-misses in production
      * Collection Method: Incident response system logs
      * Usage: Assess overall effectiveness of security program; identify areas for improvement
    - *Static Analysis Findings*
      * Description: Number and severity of issues found by static analysis tools
      * Collection Method: Automated reports from Cppcheck, Clang Static Analyzer, and SonarQube
      * Usage: Track code quality trends; identify common security mistakes
    - *Penetration Testing Results*
      * Description: Number and severity of vulnerabilities found during penetration testing
      * Collection Method: Annual third-party penetration testing reports
      * Usage: Assess real-world security posture; prioritize security enhancements
* **Security Team Roles and Responsibilities**
  + The security team at A Pet Nose Best plays a crucial role in ensuring the effectiveness of our software assurance program. Here are the key roles and their responsibilities:
    - *Chief Information Security Officer (CISO)*
      * Overall responsibility for the company's security strategy
      * Approves software assurance policies and guidelines
      * Reports on security status to executive management
      * Ensures alignment between security initiatives and business objectives
    - *Security Architect*
      * Designs and maintains the overall security architecture
      * Reviews and approves major architectural decisions
      * Develops and maintains secure design patterns and reference architectures
      * Conducts threat modeling sessions for new features and products
    - *Application Security Engineer*
      * Develops and maintains software assurance guidelines
      * Conducts security code reviews
      * Manages and configures static analysis tools
      * Provides technical guidance to development teams on security best practices
      * Assists in troubleshooting and resolving security issues
    - *Security Operations Analyst*
      * Monitors security events and alerts
      * Conducts initial triage of potential security incidents
      * Manages and maintains security information and event management (SIEM) systems
      * Performs regular vulnerability scans and analyzes results
    - *Penetration Tester*
      * Conducts regular penetration tests on applications and infrastructure
      * Identifies and reports on security vulnerabilities
      * Provides recommendations for remediation
      * Assists development teams in understanding and addressing found vulnerabilities
    - *Security Awareness and Training Coordinator*
      * Develops and delivers security training programs
      * Manages the continuous learning platform for security education
      * Tracks completion of mandatory security training
      * Organizes security awareness campaigns and events
    - *Compliance Specialist*
      * Ensures software assurance practices meet relevant industry standards and regulations
      * Conducts internal audits of security practices
      * Prepares documentation for external security audits
      * Keeps the team informed about changes in compliance requirements
    - *Incident Response Coordinator*
      * Develops and maintains the incident response plan
      * Coordinates the response to security incidents
      * Conducts post-incident reviews and ensures lessons learned are incorporated into practices
      * Manages relationships with external incident response and forensics providers