Product Information

Product Name:	Hiroko Vasquez
Organization:	Pearson and Huffman Traders
Client:	mahek (xateh@mailinator.com)
Assessment Date:	August 18, 2025

Questionnaire Responses

Build and Deployment

Q1: Do you have a defined and documented build process?

Answer: D) All teams follow a consistent, well-documented process.
Score: 4.0/5.0
Comments: Odio ex quo reprehen

Q2: Are your builds and tests performed in isolated environments?

Answer: E) Advanced security checks and isolation methods ensure scalability and performance.
Score: 5.0/5.0
Comments: Nisi officia tenetur

Q3: Are artifacts signed to ensure integrity and authenticity?

Answer: C) Most artifacts are signed, but verification is inconsistent or manual.
Score: 3.0/5.0

Q4: Do you have a defined and documented deployment process?

Answer: B) Some teams follow a deployment process, but it is undocumented and inconsistent.
Score: 2.0/5.0
Comments: Ad ullam aliquam ut

Q5: Do you use rolling updates during deployment to minimize downtime?

Answer: B) Rolling updates are occasionally used but not consistently.
Score: 2.0/5.0
Comments: Omnis dolor pariatur

Q6: Are artifacts built once and deployed across all environments?

Answer: B) Some artifacts are reused, but builds for different environments are still frequent.
Score: 2.0/5.0
Comments: Reiciendis ex autem

Q7: Has a patch policy been defined and implemented for all artifacts (e.g., container images)?

Answer: D) A patch policy is defined, enforced, and regularly reviewed for effectiveness.
Score: 4.0/5.0
Comments: Soluta eum maiores q

Q8: Are automated pull requests (PRs) for patching dependencies integrated into your workflows?

Answer: C) Automated PRs are integrated into workflows but require significant manual intervention.
Score: 3.0/5.0
Comments: Aliquid velit et id

Culture and Organization

Q1: Are nightly builds of base images conducted to ensure up-to-date dependencies?

Answer: D) Nightly builds are conducted, validated, and monitored for all critical base images.
Score: 4.0/5.0
Comments: Magni quidem dolore

Q2: Is threat modeling conducted at the technical feature level during sprint planning?

Answer: E) Comprehensive threat modeling is conducted consistently during sprint planning, identifying risks and guiding security improvements proactively.
Score: 5.0/5.0
Comments: Aspernatur est hic o

Q3: Are abuse stories created alongside user stories to address security considerations?

Answer: E) Abuse stories are an integral part of the development process and include comprehensive security considerations, validated by security specialists.
Score: 5.0/5.0
Comments: Aspernatur rerum vol

Q4: Are advanced threat modeling practices implemented to identify risks?

Answer: B) Advanced practices are occasionally used but are inconsistent and lack proper documentation.
Score: 2.0/5.0
Comments: Nostrum proident re

Q5: How frequently do you conduct ad-hoc security trainings for your software developers?

Answer: D) Regular ad-hoc trainings are conducted to address emerging threats and vulnerabilities.
Score: 4.0/5.0
Comments: Sequi illo nemo temp

Q6: How accessible are security consultants for your development teams?

Answer: A) Security consultants are not available for the development teams.
Score: 1.0/5.0
Comments: Asperiores exercitat

Q7: How often do you conduct collaborative security checks with developers and system administrators?

Answer: B) Collaborative security checks are rarely conducted and lack formal processes.
Score: 2.0/5.0
Comments: Qui non error simili

Q8: How well-defined and documented are your business continuity and disaster recovery (BCDR) practices?

Answer: E) Comprehensive BCDR practices are fully integrated into operations, regularly updated, tested, and optimized for rapid recovery.
Score: 5.0/5.0
Comments: Ullam quos pariatur

Q9: How thoroughly are new versions of source code or infrastructure components reviewed for security measures?

Answer: B) Security reviews are sporadic and conducted for critical components only.
Score: 2.0/5.0
Comments: Neque ut soluta alia

Implementation

Q1: How well-defined and implemented is your change management process?

Answer: D) Change management processes are thoroughly implemented, with clear documentation and organization-wide adherence.
Score: 4.0/5.0
Comments: Odit a cupidatat rep

Q2: How effectively does your organization implement contextualized encoding to prevent injection vulnerabilities?

Answer: D) Contextualized encoding is systematically applied across the application, minimizing injection risks.
Score: 4.0/5.0
Comments: Ad corporis sit reru

Q3: How well does your organization implement application hardening practices, following frameworks like OWASP ASVS?

Answer: A) No use of frameworks like OWASP ASVS for application hardening.
Score: 1.0/5.0
Comments: Qui nihil incidunt

Q4: Are versioning practices implemented to track artifacts and prevent untracked deployments?

Answer: A) No versioning practices are implemented.
Score: 1.0/5.0
Comments: Deserunt rem officia

Q5: Are branch protection measures like PRs, force push blocks, and status checks enforced?

Answer: D) Branch protection measures, including PRs, force push blocks, and status checks, are consistently enforced for all branches.
Score: 4.0/5.0
Comments: Sed in sed in conseq

Q6: Are tools like .gitignore and static analysis integrated to enhance code quality?

Answer: C) .gitignore is used, and static analysis tools are integrated into some parts of the development workflow.
Score: 3.0/5.0
Comments: Eos voluptatem Maxi

Q7: Are applications isolated in virtualized environments to prevent cross-service vulnerabilities?

Answer: B) Some applications are isolated, but many still share environments.
Score: 2.0/5.0
Comments: Omnis minim cupidata

Information Gathering

Q1: Are environments hardened using baseline security practices?

Answer: D) All environments are hardened consistently using industry-standard baseline practices.

Score: 4.0/5.0
Comments: Dolorem harum except

Q2: Is centralized system logging implemented to prevent unauthorized manipulation and corruption?

Answer: E) Centralized logging with advanced features like tamper-proof mechanisms and access controls is fully operational.
Score: 5.0/5.0
Comments: Tempor nulla dolor c

Q3: Are security-relevant events logged (e.g., login attempts, user management, input validation)?

Answer: C) Security-relevant events are logged for most systems.
Score: 3.0/5.0
Comments: Qui error voluptatem

Q4: Are logs visualized in a real-time monitoring system for easy assessment?

Answer: D) A real-time monitoring system is implemented for all logs.
Score: 4.0/5.0
Comments: Ea blanditiis enim n

Q5: Are system metrics like CPU, memory, and disk usage monitored for performance and bottlenecks?

Answer: D) Comprehensive monitoring of system metrics is implemented.
Score: 4.0/5.0
Comments: Reprehenderit incidi

Q6: Are metrics visualized in real-time for quick assessment and analysis?

Answer: C) Real-time visualization is implemented for critical metrics.
Score: 3.0/5.0
Comments: Ut ut illo voluptati

Q7: Are incidents triggered based on metric thresholds and alerts set for relevant stakeholders?

Answer: C) Threshold-based alerts are consistently configured for most metrics.
Score: 3.0/5.0
Comments: Fugit aut voluptate

Q8: Are vulnerabilities tracked by severity and communicated to relevant teams quarterly?

Answer: B) Some vulnerabilities are tracked, but communication is inconsistent.
Score: 2.0/5.0
Comments: Voluptatem in id b

Test and Verification

Q1: Is response statistics such as Mean Time to Resolution (MTTR) for patching vulnerabilities measured and communicated?

Answer: C) Response statistics, including MTTR, tracked and communicated quarterly.
Score: 3.0/5.0
Comments: Blanditiis id fugiat

Q2: Are unit tests implemented for critical security-related features like authentication and authorization?

Answer: E) Advanced unit tests are implemented, with continuous monitoring and frequent updates for new security risks.
Score: 5.0/5.0
Comments: Possimus consequatu

Q3: Is there a smoke test performed after each deployment to verify basic functionality and security?

Answer: E) Automated and optimized smoke tests validate functionality and security after every deployment.
Score: 5.0/5.0
Comments: In voluptatem assume

Q4: Are vulnerabilities identified during application tests visually represented in an easy-to-understand format?

Answer: E) Sophisticated visualizations with actionable insights are generated automatically to ensure clarity and prioritization.
Score: 5.0/5.0
Comments: Aliqua Ullamco cons

Q5: Are vulnerabilities tracked across different layers (e.g., application, infrastructure) and communicated?

Answer: E) Advanced tracking and communication processes ensure seamless coordination across layers for vulnerability management.
Score: 5.0/5.0
Comments: Occaecat cillum sunt

Q6: Are vulnerabilities prioritized for remediation based on their severity and accessibility?

Answer: B) Prioritization is ad hoc and does not fully consider severity or accessibility.
Score: 2.0/5.0
Comments: Et pariatur Ullam q

Q7: Does the vulnerability scan cover client-side dynamic components (e.g., JavaScript execution)?

Answer: E) Advanced scans with automated tools ensure full coverage of client-side dynamic components, including rare edge cases.
Score: 5.0/5.0
Comments: Excepturi enim aut s

Q8: Are multiple roles authenticated and tested during vulnerability scans?

Answer: E) Advanced practices ensure dynamic role-based testing with extensive scenario coverage.
Score: 5.0/5.0
Comments: Sed delectus do a e

Q9: Are network configurations tested to identify unintentionally exposed services?

Answer: C) Network configurations are tested regularly, but some exposure risks may remain undetected.
Score: 3.0/5.0
Comments: Eaque deserunt unde

Q10: Are cloud environments tested for configuration hardening?

Answer: D) Comprehensive tests ensure cloud configurations meet hardening standards.
Score: 4.0/5.0
Comments: Id dolorum officia

Q11: Are static analysis tools used for source code vulnerabilities?

Answer: D) Comprehensive static analysis is conducted regularly across the full codebase.
Score: 4.0/5.0
Comments: Autem et quidem nisi

Q12: Are stylistic rules and best practices enforced in the codebase?

Answer: D) Automated stylistic analysis tools enforce compliance.
Score: 4.0/5.0
Comments: Et sapiente in hic i

Q13: Are static analysis tools used for infrastructure vulnerabilities?

Answer: B) Some tools are used for static analysis of infrastructure, but coverage is incomplete.
Score: 2.0/5.0
Comments: Hic labore temporibu

Q14: Are unused resources, such as secrets, identified and removed from infrastructure?

Answer: D) Tools are used to automatically identify and remove unused resources, including secrets, from infrastructure.
Score: 4.0/5.0
Comments: Facilis dolor nostru

Q15: Are test intensity and confidence thresholds optimized to balance accuracy and time?

Answer: A) Test intensity and confidence are not considered, leading to inefficient or incomplete testing.
Score: 1.0/5.0
Comments: Odio id sed in paria

Q16: Are regular automated security tests performed?

Answer: D) Automated security tests are regularly performed with good coverage across key components.
Score: 4.0/5.0
Comments: Reprehenderit fugit

Maturity Assessment Results

Overall Maturity Score:	3.3/5.0
Maturity Level:	Level 3 - Defined
Maturity Progress:	3.3 out of 5.0 levels