DDN1 TASK 3: Technology-Supported Security Solution

Mohit Ballikar

College of Information Technology, Western Governors University

February 22nd, 2025

Technology-Supported Security Solution for Beetle Films

A. Policy Adoption with Project Implementation

With the current project implementation, security checks and compliance policies are changed to accommodate the new payment system and PCI DSS controls. Though many aspects of these technical controls should be well-understood by the security team, policy changes will also ensure that future or less-experienced employees will be informed. Though the serverless migration allows for some of the technical and administrative controls to be streamlined and improved, policies to enforce this are still relevant. AWS Config will enable policies to be implemented across the environment, providing a single pane view. The configuration applied to the accounts, buckets, databases, and other components all reflect a stringent policy per PCI DSS. Policies ensuring payment data is handled and stored securely are key in configuring within an IaaS environment, such as the one Beetle Films uses.

With rules enforced in this way, monitoring them allows for immediate understanding and response, in the case of security issues or noncompliance. The monitoring aspect of any payment-handling organization is key to reducing latency and improving decision-making. Response plans following these policies to ensure readiness and the proper training allow for low latency in operational decisions regarding security. Furthermore, communicating issues in implementing policy can be forwarded to the service provider to understand what needs to be provisioned if additional services are required.

In drilling down into the specifics of the established policies for Beetle Films, one can begin with the data encryption and protection-based policies that would be

established. As stated by the name, the key focus of this would be for integrity and confidentiality to be maintained for the organization. The utilization of encryption-at-rest for the S3 bucket storage and databases allows for PCI DSS compliance and user-data security (PCI Security Standards Council, 2018). TLS enforcement is key to restricting traffic to secure channels in handling in-transit data communications. The lack of in-transit data encryption would ease on-path attacks, which can be forced through API gateway communication (AWS WAF from the network perspective) and AWS CloudFront for certificate or user termination. Lastly, to reinforce on-path defenses, as well as insider leaks, the tokenization of payment card information throughout aspects of the operation will be implemented. This can be done independently by Beetle Films' development team through their application changes, or the reliance on AWS Payment Cryptography service can be leveraged. However, this may be over-implementation in the early phases.

In rotating from technical to administrative controls, in further describing implementation policies, least privilege is an explicit control that applies to Beetle Films' new environment. The monitoring and evaluation of accounts to align with the principle of least privilege is key in ensuring no account receives any level of privilege creep. In situations where elevation is required for specific roles, temporary account elevation will be enforced, and policies to limit access to administrative accounts are key (NIST, 2023). Multi-factor authentication will be established to maintain stringent access control when authenticating internal, administrative, or external user accounts. The aforementioned use of AWS Cognito will catalyze this process first-party through AWS' services. Strict authentication mechanisms through this medium will be required

internally. However, community user accounts will only be required to use MFA if they are paying supporters of the platform to provide another level of security to their accounts. Lastly, rule-based access control within both the internal accounts and forum-interacting user accounts will be implemented to tier account controls and provide a more granular level of access throughout the platform (NIST, 2023). The aforementioned administrative accounts are an example of this, with their time-limited access specific to that role. However, the tiering of paying subscriber accounts versus regular user accounts on the forum allows for the earlier MFA controls to be more focused.

In overseeing many of these administrative and technical controls, monitoring and logging policies must be in place to establish and maintain a baseline within Beetle Films. With the centralized approach to events and metrics (with AWS CloudWatch, CloudTrail, and AWS Config), monitoring aggregation will allow for speedy response and delegation in incident scenarios. The primary purpose of this policy within the implementation of the solution is to enforce real-time detection and response throughout the infrastructure, aligning with PCI DSS compliance (PCI Security Standards Council, 2018). Automated detection and response configurations from AWS Config and GuardDuty will update platform posture metrics as often as necessary. Through this policy, mitigation measures for anomalous or fraudulent access will dramatically reduce the possibility of compromise.

In following within the vein of response and monitoring capabilities, the incident and recovery policies will apply to ensure events are handled appropriately without disrupting operations significantly. Establishing a backup policy (through the AWS

Backup service) tailored to daily backups and weekly retention periods will ensure Beetle Films' availability (PCI Security Standards Council, 2018). The specific metrics are stressed to align with PCI DSS compliance and general best practices in dealing with breaches or incidents. Leveraging and updating playbooks for incident scenarios will ensure that standardized responses are being taken. This practice established within the policy will ensure that preparedness is maintained for the organization. Runbooks automating portions of this document can expedite detection and recovery metrics, though proper configuration is foremost. Lastly, establishing a general recovery time objective of 4 hours and a zero loss of data recovery point objective can point efforts in resolving these issues quickly and effectively (from backups). In the latter sections, the flexibility of this rule is described further, as some incidents/issues may be advanced and persist much longer. The provisioning of new systems/resources to replace affected components is much quicker, though the complete forensic analysis of lessons-learned protocol would be more appropriate for more complex and impacting incidents.

In correlating all aspects of these policies with Beetle Films' operational requirements, auditing and testing are relevant in maintaining compliance under industry/regulatory standards. Approved scanning vendor testing is required to uphold Beetle Films' PCI DSS compliance. This must be done every 90 days (once a quarter), ensuring adherence (PCI Security Standards Council, 2018). Internally, leveraging the aforementioned monitoring tools can allow for automated compliance reporting, providing the platform with a continuous understanding of security posture and alignment. In addressing development risks, the enforcement of DevSecOps and

dependency management will audit and minimize this possible attack surface (NIST, 2023). Due to this policy, OWASP Top 10 scans carried out regularly would provide a deeper understanding of possible vectors within applications.

In summation, the above policies address the various aspects of security, compliance, and operational concerns for Beetle Films. Streamlining and establishing protocols through these policies will improve decision-making within the implemented environment. With many of the provisioned tools and services at hand, Beetle Films will have a holistic solution in dealing with the issues of the past infrastructure. Specifically, automation and centralization from the adopted policies will enforce a secure baseline for business operations, which can be improved and optimized when necessary due to the IaaS model's flexibility.

B. Cybersecurity Assurance Criteria Compliance

In defining the solution in the context of cybersecurity compliance, we can see the direct needs for modern security that borrows from industry-standards and regulations that the transition was designed around. In addressing automation in cybersecurity operations for Beetle Films, the monitoring and analysis provided by many AWS tools can simplify peering into the current posture. Active monitoring is also requirement under NIST and PCI DSS standards, but the ideal single pane approach from this setup allows for greater ease, and in turn, automation. Runbooks allow for any complications to be solved through this minor automation, reducing the human hours needed to process events. Using a SIEM in this situation also summarizes the endpoint, component, and user auditing to provide a greater depth for this data.

With this solution, the aforementioned single-pane and automation approach is a clear benefit in improving and modernizing the security posture of Beetle Films. The features within AWS Security Hub/AWS Config allow for the implementation of the earlier automation and ensuring misconfigurations are dealt with efficiently. The updateable and growing requirements that the payment industry calls for, can be met using tools like these, within the AWS environment. Compared to the less streamlined and more manual security methods in Beetle Films' past, these features show a clear improvement for the organization. The inclusion of tools to accommodate this new platform (e.g. Terraform) are also open-source and more modular, the end-of-life components before the migration would require significant effort and monitoring only to fail future PCI DSS audits. The new posture provided by proposal and planning will allow Beetle Films to evolve and modernize their operations, security and responses can be provisioned appropriately going forward. Content distribution networks (CDNs) can allow for even larger scale reach, further modernizing the once cult-classic platform.

In tying aspects of the proposed solution back to industry standards, the aforementioned constant monitoring is clear with the new auditing capabilities within the AWS suite. Specifically, CloudWatch and GuardDuty will allow for immediate response and auditing when PCI DSS anomalous activity is concerned. The general threat detection is required under the earlier standards but also key in ISO 27001, to ensure that security monitoring is in place, especially for sensitive data processing. Availability concerns stemming from industry requirements (specifically for sensitive payment data) are solved through AWS Backup and the scaling features to meet requirements for ideal operational scenarios. In conjunction with insurance policies in the far future if Beetle

Films is in a much more impacted position, would reduce concerns significantly. The secure configurations of the IaaS model are also ensured to be in line with Zero Trust needs, segmentation and IAM policies will greatly reduce the outlying attack surface of the organization. The authentication concerns are also relieved in part to the use of AWS Cognito, providing MFA, also strengthening the posture towards PCI DSS.

The migration to the new serverless infrastructure captures many of the modern and secure industry tools that Beetle Films would benefit from, as described in the proposal. The configurations established by the cloud security architect contracted, in conjunction with the expansion of security principles to the development team, Beetle Films should be more than capable of processing payment information and passing security audits.

C. Data Collection and Implementation Elements

Data collection and monitoring must exist for analysis in complying with the ideal standards and regulations regarding payment information. Auditing traffic and transactions within Beetle Films' infrastructure allows them to have transparency with their operations. The collection and auditing of this data is facilitated through the aforementioned CloudTrail and Config services that AWS offers. The collection and review of this data is automated to the extent of notifying analysts of flags or events of interests. The immutability of these logs and event-tracking tools ensures that future scenarios of forensic analysis are possible. Immediately event management is streamlined, following playbooks, but reporting the data remains as needed. The collection and storage of these logs upon longer instances of time, can be included

within the AWS Backup provisions, though no minimum period exists concerning PCI DSS requirements.

The monitoring and collection aspects above directly aid in enforcing integrity to the Beetle Films' users/supporters. In tracking traffic and sensitive data-use, for security, the posture of Beetle Films' can be responded to and communicated to stakeholders in the event of an incident. The associated plans and playbooks regarding these events further strengthen the response capabilities of integrity-harming events, for processed data. Incidents impacting the organization may also pertain to the other two tenets: confidentiality and availability. The concerns seen within the proposal for Beetle Films, all three tenets are in consideration. Availability surrounding the service operations is maintained through scaling provisions, this can extend to simple storage and compute for film-hosting, backup increases, or overhead scaling. The level for scaling/provisioning components within Beetle Films will be following the cases detailed in playbooks and response plans, and possible consultation from AWS officials, in extreme situations. Confidentiality and integrity are supported hand-in-hand with secure end-to-end encryption and storage. The human issue can also be addressed here with the tokenization of this data in auditing and tracking to keep things as zero-trust as possible.

The alignment of data for continual monitoring, processing, analysis, and CIA triad tenets ensures that the security posture of Beetle Films is secure to the best of the organization's capabilities. Industry standards such as PCI DSS and the NIST special publications aid to guide and benchmark the preparation of each of these components. Lastly, the integrity of the organization and management is necessary to uphold these

design principles and ensure that users and stakeholders are considered and safe. The attack surface and likelihood are generally low, though due diligence is a must.

D. Cybersecurity Crime Investigation and Mitigation

The proposed solution mitigates crime and incidents through the tools listed earlier as well as the training in place for personnel. The constant monitoring, coupled with response plans, allows for immediate courses of action. Training and keeping employees up to date with awareness and understanding of risks and actors can go a long way in reducing the attack surface for the organization. This will also allow for quick and prepared lines of action in the event of an emergency or incident. The security team receiving further training to specialize roles within incident response should keep all roles/stakeholders involved and aware when the time comes. The use of anti-phishing measures will allow for social engineering measures to be mitigated over time. The crimes respective to PCI DSS compliance are mostly stemming from issues with IAM or zero-trust.

The tokenization of sensitive data, within internal logging, reduces the likelihood of an insider threat through leaks. Limiting access to handling such data to MFA required access, as well as ensuring nonrepudiation, can definitively label malicious insider access or compromise. Policy for password and access measures to be stringent and in line with industry standards can also mitigate the possibility of a threat to the organization through account compromise, these authentication/access control measures can also extend to community/users of Beetle Films. This will further limit the

attack surface of the organization and the vectors to access the sensitive payment information.

Technical controls in mind, the reiterated monitoring tools within the AWS suite serve to meet and continue PCI DSS compliance and in turn, eliminate the possibility of cybersecurity criminal threats. Trend analysis, whether traffic or behavior, can provide baseline understanding of when anomalies occur that may signify threats or crimes. With the proper playbooks and preparation, in Beetle Films' new infrastructure, mitigative measures can always be improved and implemented. In the pre-migration infrastructure, issues surrounding streamlined auditing and hardening can arise due to the end-of-life nature of the servers/components.

E. Plans, Standards, and Procedures For the Solution

The issue at hand for Beetle Films was their older infrastructure not being able to keep up with PCI DSS compliance and scaling demands with community growth. The solution to remedy this is within the transition to a serverless architecture hosted by AWS, within this new environment the security tools/services offered by AWS will be leveraged according to best practices and PCI DSS compliance. This clearly follows needs for compliance, cybersecurity initiatives are clear as well with the training and planning in place. Elevating awareness throughout the organization in preparation for sensitive data handling, establishes readiness and lowers the surface for social engineering attacks/compromise. The reiterated access control and auditing requirements called for by best practices and PCI DSS allow this preparedness to be

tested and certified, proving operations to be safe. MFA and secure data transmission/collection limit access to data processed.

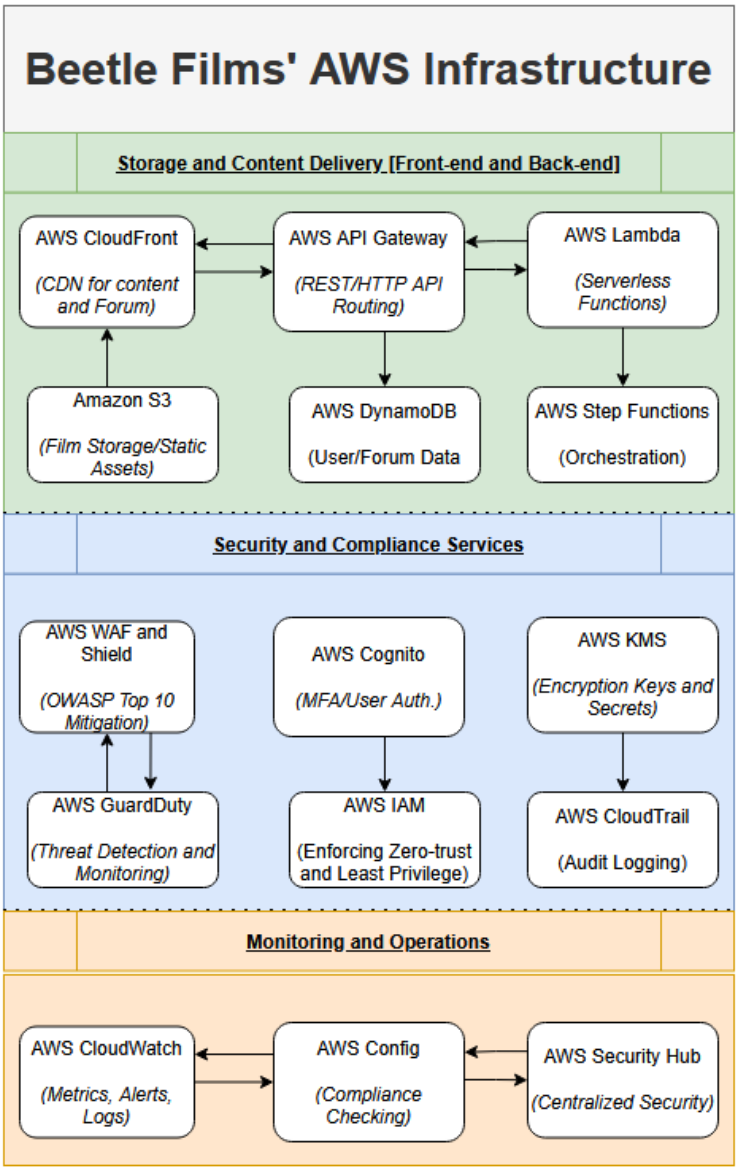
In relating all of these precautions, measures, and components, plans and procedures utilizing them must exist to create a safe and controlled environment for business operations. The incident response planning involving the security team, administration, owners, possible regulators, and AWS contacts as stakeholders keeps all parties informed and involved when necessary. Within the security team, a smaller subset possesses responsibilities beyond other security analysts/engineers, being the first to respond and monitor incidents, if they were to appear. With the close-knit, smaller scale of human capital within Beetle Films, the owners/administration are involved when possible, and act in place for human resources officials in addition to their higher-level responsibilities. For incidents involving other parties, for either provisioning or reporting, then the administration will communicate these needs to the respective parties, after checking in with the owners of the platform first.

In situations of continuity planning for the organization, most of the decisions and planning are done internally by the owners/administrators. The bootstrap approach they once had with the platform being much smaller has given them a jack-of-all trades insight, however certain instances such as the migration of Beetle Films here, may be better guided or handled by third-party agents/contractors. Policy stemming from this is security-first, as the platform values users, content-providers, and regulators. With the current consumer-base there should not be any gaps in understanding in viewing and using the new serverless platform, as the front-end will be unchanged for a period.

Extending policies of MFA, high entropy passwords, and privacy-concerns (mitigating social engineering) to the user-base will require some minor guidance as the demographic of viewers/users changes and increases. Informing this new information would be done directly upon login, and a prerequisite for the higher tier forum supporters who will be paying a monthly subscription to Beetle Films (to ensure user-safety is established before sensitive data is inputted). The details of this tiering will be announced upon the release of the new platform, but the perks will generally be cosmetic to highlight support for the platform. This minor detail will justify the secure transition, with autoscaling resources also in mind, PCI DSS compliance is a must.

The tooling/training intended to be used with the solution (and its implementation) is mostly from third-party entities, for the internal workers at Beetle Films. AWS's Skill Builder was intended to be leveraged to increase knowledge on the workings of their proprietary tools/services. Though some individuals within the security and development team have strong backgrounds, especially in serverless tooling/architecture, supplementing this information on-demand through this service can ensure that knowledge gaps are addressed (Amazon Web Services, 2024). Guidance will also be provided during the initial setup, in correspondence with AWS agents to ensure the support and provisioning is in line with what is expected. The utilization of these IaaS provisions will be dictated by the administration of Beetle Films and the contracted cloud security architect. Overall, the planning and procedures follow best practices associated with PCI DSS, with specific implementation details defined within the artifact. The playbook capitalizing from this will streamline the internal response in operations for Beetle Films.

F. Post-Implementation Environment



The diagram above illustrates the makeup of the infrastructure provisioned by Beetle Films, with the proposal in mind. The storage and content delivery components of the new infrastructure allow for on-demand scaling, with granular IaC control, which aligns with Beetle's long term growth goals and compliance goals. As reinforced throughout this document and the earlier proposal, the needs for security (MFA,

auditing, etc.) are represented within the bottom two categories. Without this implementation utilizing AWS services, the organization may have issues with serving content securely in the past, inhibiting them from growing and monetizing. Posture-wise, the transition to newly updated services that will share some responsibilities with AWS is much improved over the earlier end-of-life systems. The alternative to this implementation, with the prior infrastructure in mind, would be to eventually create custom-patches for the servers, if compromise were to occur then redundancy is not available, not to mention scaling due to the limited nature of the servers. Overall, this serverless solution allows for a brighter future for Beetle Films, without as much overhead and responsibility in managing it.

PCI DSS Penetration/Vulnerability Status Report

Requirement	***Status***	***AWS Control***	***Evidence***
3.4	Pass	S3/RDS encrypted with AWS KMS.	AWS Config rule "*s3-bucket-server-side-encryption-enabled*" shows compliance.
4.1	Pass	TLS 1.3 enforced via CloudFront/API Gateway.	CloudFront viewer protocol policy set to TLSv1.2–1.3.
6.6	Pass	AWS WAF blocks SQLi/XSS attacks.	WAF logs show blocked OWASP Top 10 requests.

8.3	Pass	MFA is enforced for all required users via AWS Cognito.	Cognito user pool configured with TOTP/SMS MFA.
10.1	Pass	CloudTrail logs enabled and centralized.	CloudTrail trails configured for all regions.
11.2	Pass	Quarterly scans conducted via Nessus/AWS Inspector.	Scan reports dated for April 2025.

With the above vulnerability report in mind, we can see the new processes and services in place to ensure that security and compliance are in mind for Beetle Films. This will allow for the desired operations to execute, as the revenue of forum supporters is accessible (securely) as shown above. Processes for Beetle Films should be relatively unimpacted as the controls in place will require monitoring and tweaking on occasion, but this is a far lower workload than projected from the pre-migration infrastructure. The throughput and performance are detailed further below.

Infrastructure Performance Report				
Metric	***Current Measurement***	***Target at 30,000 Users***	***Status***	***Comments***
API Gateway	150	900	Pass	AWS API

Request/Second	Requests/second	Requests/second		Gateway scales to 10,000 RPS by default. No throttling observed.
Lambda Concurrency	50 concurrent executions	300 concurrent executions	Pass	AWS Lambda scales automatically; concurrency limit raised to 1,000.
CloudFront Cache Hit Ratio	92%	≥ 85%	Pass	High cache efficiency for static assets (films, CSS, JS).
Film Streaming Latency	200ms (avg)	≤ 500ms	Pass	S3 + CloudFront can 4K films with low latency globally.

DynamoDB Read Latency	15ms	≤ 25ms	Pass	Provisioned capacity with auto-scaling enabled.
Forum Response Time	800ms	≤1,500ms	Pass	Serverless architecture handles spikes; optimized Lambda cold starts.
Server Error Rate (5xx)	0.2%	≤ 1%	Pass	API Gateway retries, and Lambda error handling reduce failures.
Data Transfer (Monthly)	500 GB	3 TB	Pass	CloudFront reduces origin load; S3 Intelligent-Tiering optimizes costs.
Uptime (SLA)	99.95%	99.90%	Pass	Multi-AZ RDS and S3 cross-

				region replication ensure high availability.

The performance of the new environment is also of concern, though this is not as audited as the security controls, services, ensuring performance can keep up with user growth over time can aid to offset the initial cost of the migration. This is valuable in guaranteeing the content providing stakeholders and the relying community receives the services they need from Beetle Films. The licenses/permissions received from content providers are only dependent on a community receiving the content in a reliable manner, providing exposure and discussion around the works. The metrics also consider the efficacy of Beetle Films' internal teams in migrating and establishing the new infrastructure, though this is relatively streamlined with the aforementioned aid of the cloud security architect. These provisions/tests will provide a large increase in traffic to the platform as well as revenue, with support from the community. Overall, the prior report on security ensures that these performance metrics are not compromised by possible threat actors, and that security measures are in place to protect sensitive customer data. These components are definite business process improvements.

The summative evaluation plan consists of ensuring that infrastructural performance is within the necessary standards and goals. The auditing requirements for PCI DSS are forefront in any testing for the organization, as scaling and performance can be implemented in the future due to the IaaS nature of the new platform. The performance results for load-testing in post-implementation for release along with

compliance results are listed in the above reports. In addition, summative testing for disaster recovery/business continuity, and feedback testing are valuable. The former just puts procedures into practice for incident response and availability maintenance, to ensure that security is upheld as well. Below is a table outlining the procedure for beetle Films dealing with a threat actor in this new environment.

Incident Response Playbook			
Phase	***Key Actions***	***Tools/Resources***	***Timeline***
Preparation	- Deploy AWS Config/Security Hub. - Train teams on PCI DSS requirements.	AWS Trusted Advisor, Nessus, Incident Log (Confluence).	Ongoing
Identification	- Trigger alerts via AWS Config/Security Hub. - Categorize severity (Critical/High/Medium).	AWS CloudTrail, AWS GuardDuty.	≤ 15 mins
Containment	- Quarantine noncompliant resources (e.g., block S3 public access). - Preserve logs.	AWS CLI, AWS WAF.	≤ 1 hour
Eradication	- Fix root cause (e.g., update IaC, patch	Terraform, AWS Cognito (MFA).	≤ 4 hours

	systems). - Re-deploy resources.		
Recovery	- Validate compliance via AWS Config. - Restore from backups if needed.	AWS Backup, Nessus.	≤ 24 hours
Communication	- Notify CISO/Legal. - Report to PCI SSC if breach confirmed.	PCI Portal, Internal Slack/Email.	≤ 1 hour
Post-incident	- Conduct RCA. - Update playbook/docs.	AWS CloudTrail, Jira/Confluence.	≤ 72 hours post-fix

The general layout of the incident response playbook is as listed above. The results of following simulated incidents and training were within the acceptable range of operation. The current employees responsible for incident response are experienced, but the desired metrics may not be as easily reached as new talent is added to Beetle Films. The supplemental training and assistance within the security team should allow for any gaps, even in the long-long-term to be addressed. The recovery capabilities listed within this procedure are also supported by the performance report above.

Lastly within summative testing, the feedback and reception from relevant stakeholders had to be considered as well. Internally, the concern of reaching performance metrics and compliance standards were in primary focus. Externally, the

compliance auditing/pen-testing concerns were met with the passing report results. The only external feedback from a small test group of users was to have the front-end/interface of the platform updated. This will be addressed once Beetle Films rolls out to the public by the development team. The other portions of summative testing, recovery/incident response are within parameters for successful operations, though deviances will mostly rely on optimization by the Beetle Films teams. This can be from the implemented controls to the administrative plans for incident/disaster response. Any additional weaknesses or deficiencies that may arise, that cannot be solved in this manner, will need to be provisioned. This can include higher throughput/service-level from AWS or external contractors/aid.

In addressing risks in the post-implementation phase for Beetle Films, the main concerns are insider threats and social engineering (for the user community). Currently, the insider threat concerns are relatively unlikely due to the close-knit and trusted nature of Beetle Films' employees. The impact of compromise is reputational, monetary, and possibly legal. Fines and legal costs combined can set the organization back as far as one million dollars depending on the severity of the insider damages and the length (PCI Security Standards Council, 2024). The one-time fines for this threat can be at minimum, $20,000 which is a significant value when the mitigative measures are a fraction of the cost (PCI Security Standards Council, 2024). In mitigating this, internally, stringent IAM controls must be in place to limit unnecessary access, this will be monitored carefully by the security team and the associated services (AWS IAM, AWS Security Hub, AWS Configuration). In long-term, as talent comes into the organization, vetting and limiting new employees’ access is necessary. Overall, in conjunction with

MFA and data tokenization, nonrepudiation will be established, as only the security team could have the possible expertise to revoke and steal the tokenized data, if monitoring were not in place. Though minor, social engineering training and preparation is also established within the organization to limit coercion efforts, from internal employees or external threat actors.

In analyzing the possibility of an external user/consumer facing compromise of their account, mitigative measures are already established to remediate portions of this risk. The utilization of MFA for payment-providing users and optional use for other users should allow for restrictive and authenticated access. Furthermore, the high entropy password policy ensures that brute force methods are also very unlikely. The likelihood of user manipulation through social engineering is minor, and at most moderate, though a larger applicability is present for the aforementioned internal staff, due to the wider range of access. The monitoring aspect mentioned above, in conjunction with the incident response playbook, will ensure that anomalous/fraudulent activity is detected and dealt with quickly. Lastly, the impact of customer compromise is parallel to the internal threat risk, with monetary, legal, and reputational damages in consideration. Though with the external perspective of a user of Beetle Films, operational damages with regard to traffic are possible, due to reputational issues. Internally, operational damages may be caused by purposeful mishandling of services/tooling, but reputational aspects can be kept private.

The security solution meets the needs of each stakeholder, with the general shared need here being the security and efficiency in processing payment information. To start with the internal security team, the serverless architecture and tooling allows for

granular monitoring and configuration controls, which would need to be specialized with considerable overhead in the prior infrastructure. The need of establishing a secure, monitored environment for Beetle Films is more than met for this group. The measures provisioned were carried out with security foremost to ensure operations can grow and evolve, while still keeping security in mind. PCI DSS compliance in addition to operational security are possible due to the serverless architecture solution, this is even catalyzed with the aid of the contracted cloud security architect (during implementation) and with supplemental training.

The internal development team benefits from the new solution as well, though not as greatly as the security team. The older infrastructure, prior to the migration, had a growing attack surface but was still operational (metric-wise) if growth was relatively limited. The platform would suffer throughput issues in serving content to a growing community, the scaling and granularity of the IaaS environment allows for the development team to provision and optimize whatever is necessary with freedom. The granularity allows for segmentation throughout the application environment and security preservation, even in scaling situations. The preexisting expertise of the team regarding serverless architecture allowed for the implementation and testing to be relatively smooth. The need of a capable development playground for the team was essentially realized through this solution.

Lastly in the perspective of internal stakeholders, the owners and management of Beetle Films had the primary desire to expand operations securely for the platform. The ingestion of payment information due to their forum supporter tiers would require all the necessary due care and diligence. This new feature, when implemented and monitored

securely by the respective internal teams, allows for community growth and additional capital to operate. The prior business model of hosting media (films) to a relatively small, cult-following was maintainable, but larger plans are forecasted for the organization. This would not be possible without dependable revenue stream as well, regardless donations from the community were not desired without something at least minor in return. The proposal drafted in *Task 2* follows the needs of management and the platform owners, the scaling and security for the cost is too good of deal to pass up.

The external auditing parties (for PCI DSS and consumer safety) share the similar needs as the security team, certifying a secure environment exists within Beetle Films to process the incoming sensitive information. The earlier reports for vulnerabilities/penetration and performance uphold the needs for compliance. Even further, the CIA triad is preserved in this new environment, an implementation concern with the new responsibility taken upon Beetle Films. The concern of future penetration and auditing, to continue certified compliance, is in the long-term consideration of management.

The content providing parties for Beetle Films are also a valuable stakeholder, when addressing needs as they essentially control the supply chain for the platform. Their needs are mostly dependent on content availability and integrity maintenance. The permissions given to the platform are contingent on a community receiving and providing feedback on the content, films primarily. The performance metrics and state-of-the-art controls within the new environment are more than enough to justify continued support for Beetle Films from this party's perspective. Moreover, the growth of the

platform, as predicted by internal management, is sustainable and beneficial for more content providers to sign off on having their films hosted on Beetle Films.

The final stakeholder party involved in the community of users for the platform itself. Their needs are mostly tied to continual performance and availability from Beetle Films, as downtime issues (from migration or security) would damage the perception of the platform. Though not fully aware of the new post-implementation benefits, regarding monetization, the secure transaction and control of this data is in best interests for both the platform and its users. The performance increases and infrastructural changes also allow for better service quality and future improvements regarding content on the platform. Overall, all stakeholders' needs are met with this serverless solution, but the needs of the community are the main drivers, as they helped to build the platform with their support.

G. Post-Implementation Maintenance Plan for Solution

The post-implementation maintenance plan stems from upholding security best practices, standards, and compliance. The continuous monitoring/enforcement controls in place within the AWS environment will allow for constant posture checking and configuration. In scaling needs, the current provisions should be more than enough for the near future, 30,000 concurrent users are in the end of the possible growth for the platform. The major maintenance is with PCI DSS compliance, in annual ASV testing. Trusted Sec may continue to certify the posture of Beetle Films, though contingency firms may also be considered. The userbase of the organization also required its own level of maintenance, in this phase of post-implementation. Feedback and changes

requested through the forum (or other methods) must be taken into consideration to continually uphold the service-level/features of the platform.

In addition to the general housekeeping of maintaining security posture and operational standards, internal training and preparation must continue. Anti-phishing measures and IAM oversight must be carried out to limit insider attack vectors. With leveraged AWS security tooling, the main attacks to consider (outside of zero-days or gross misconfiguration) will be social engineering-based. In catalyzing this, maintaining a relationship with AWS in ensuring provisions, payments, and service-levels are at the agreed upon values in also key. The shared responsibility of infrastructure in Beetle Films will continue to be communicated, and/or altered, once operations are established over the coming months/years.

H. Original Artifact

Beetle Films Incident Response Playbook

Preparation Phase:

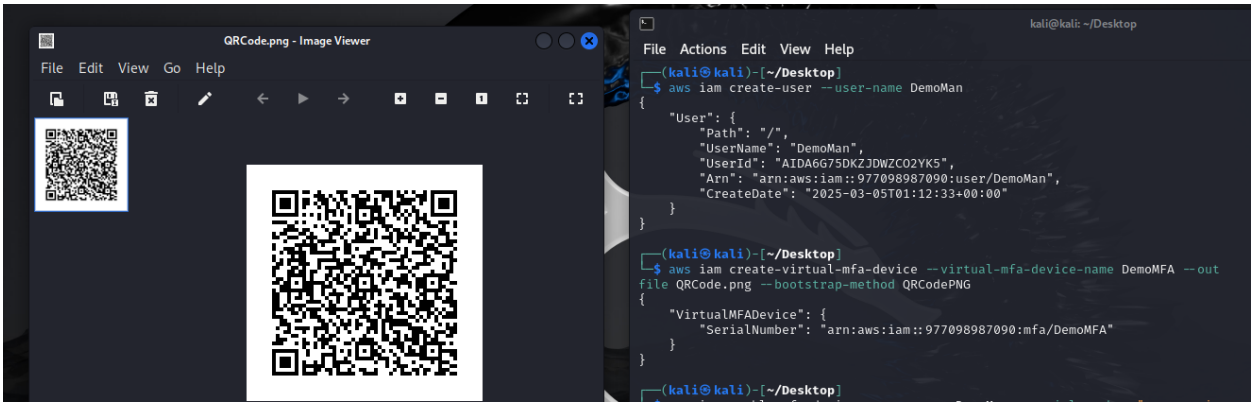
In preparing for the possibility of incidents impacting the organization, due care and diligence must be carried out at all times to ensure that maximum preparedness is in place. AWS Security Hub and Config rules must be established and monitored. The tooling throughout this process is mostly implemented in accordance with the needs of *Task 2's* proposal. The policy requirements will be aligned with NIST SP best practices and PCI DSS compliance requirements. Training staff, and supplementing knowledge where necessary, is a key feature in reducing the social threat attack surface. One major feature that will be monitored and established within these requirements is the

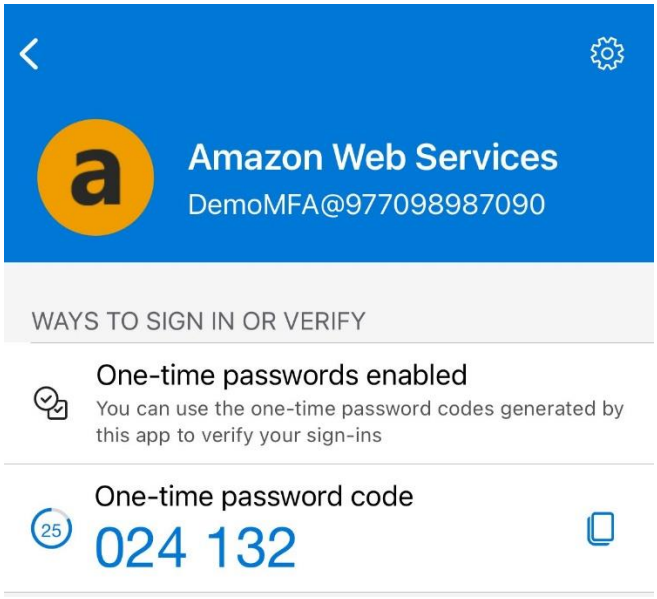
enablement of MFA for all internal accounts and payment-handling customer accounts. The specific tooling for this process will be utilizing AWS CLI and AWS IAM to set-up and apply this security control to the respective accounts. Below you can find a brief walk-through of this procedure, in initial enablement, revocation, and testing.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ aws configure
AWS Access Key ID [None]: AKIA6G75DKZJG43YYCUM
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:

┌──(kali㉿kali)-[~/Desktop]
└─$ aws iam create-user --user-name DemoMan
{
    "User": {
        "Path": "/",
        "UserName": "DemoMan",
        "UserId": "AIDA6G75DKZJDWZCO2YK5",
        "Arn": "arn:aws:iam::977098987090:user/DemoMan",
        "CreateDate": "2025-03-05T01:12:33+00:00"
    }
}
```

The creation of a user through AWS CLI provides the necessary information to then go forward and establish MFA. With this being a demonstrative account, no specific group ties are given to this user.





In creating a virtual qr-device for this user, an alternative authenticative measure is established, and must be associated with the "DemoMan" user. With this being a proof-of-concept and not a fully scaled solution, the qr code and information would be emailed to the associated users, instead of generated (locally).

```
┌──(kali㉿kali)-[~/Desktop]
└─$ aws iam enable-mfa-device --user-name DemoMan --serial-number "arn:aws:ia
m::977098987090:mfa/DemoMFA" --authentication-code1 244906 --authentication-c
ode2 317352

┌──(kali㉿kali)-[~/Desktop]
└─$ aws iam put-user-policy --user-name DemoMan --policy-name RequireMFA --policy-document file://mfa-policy.json

┌──(kali㉿kali)-[~/Desktop]
└─$ aws iam create-access-key --user-name DemoUser
{
    "AccessKey": {
        "UserName": "DemoUser",
        "AccessKeyId": "AKIA6G75DKZJPPT5NSRK",
        "Status": "Active",
        "SecretAccessKey": "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",
        "CreateDate": "2025-03-05T01:20:57+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop]
└─$ aws configure --profile DemoUser
AWS Access Key ID [None]: AKIA6G75DKZJPPT5NSRK
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

The above snippet shows the association of the generated MFA device to the created user; generated MFA codes are used to synchronize the user to the authentication method. The assignment of a user-policy is then applied, in this proof-of-

concept, the main permission concerns administrative functions such as peering into provisioned resources and account details. The account is reconfigured briefly to reset the access token, to highlight non-MFA access.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ aws iam create-access-key --user-name DemoMan
{
    "AccessKey": {
        "UserName": "DemoMan",
        "AccessKeyId": "AKIA6G75DKZJHVKXBDP3",
        "Status": "Active",
        "SecretAccessKey": "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",
        "CreateDate": "2025-03-05T01:30:27+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop]
└─$ aws configure --profile DemoMan
AWS Access Key ID [None]: AKIA6G75DKZJHVKXBDP3
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:

┌──(kali㉿kali)-[~/Desktop]
└─$ aws s3 ls --profile DemoMan

An error occurred (AccessDenied) when calling the ListBuckets operation: User: arn:aws:iam::977098987090:user/DemoMan is n
ot authorized to perform: s3:ListAllMyBuckets with an explicit deny in an identity-based policy
```

With the reconfiguration of the account and its associated access tokens, access is denied to peering into the S3 bucket contents/directories (though for this example they are empty).

```
┌──(kali㉿kali)-[~/Desktop]
└─$ aws iam get-user
{
    "User": {
        "Path": "/",
        "UserName": "DemoMan",
        "UserId": "AIDA6G75DKZJDWZCO2YK5",
        "Arn": "arn:aws:iam::977098987090:user/DemoMan",
        "CreateDate": "2025-03-05T01:12:33+00:00"
    }
}

┌──(kali㉿kali)-[~/Desktop]
└─$

┌──(kali㉿kali)-[~/Desktop]
└─$ aws s3 ls

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Upon reauthenticating with the user authentication method, access is available for user details and provioned resource details. These features are also available to be done through the GUI and web interface through AWS, though for the purpose of understanding (step-by-step) the CLI terminal and commands were highlighted. In the case of Beetle Films, scripting account creation and security features at a larger scale, based on endpoint response is much more appropriate. The creation and monitoring, as reiterated, is ongoing throughout all aspects of business operations (even in incident events). Vulnerability scanning and anomaly detection are also streams to be considered throughout this phase, as well as latter phases, but can provide preliminary timeline and RCA information later on.

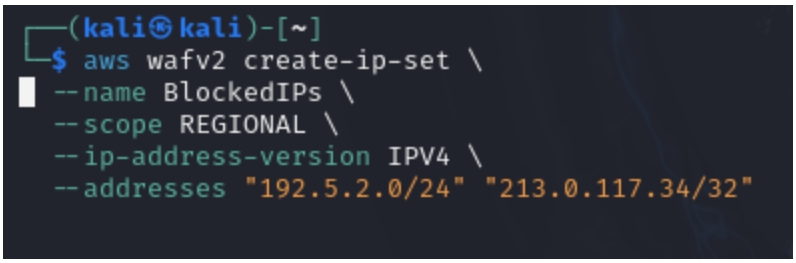
Identification Phase:

Continuing from components in the earlier phase, once the ingestion and labeling of malicious/anomalous behavior is picked up the following response must be swift. This of-course will rely on the granular and accurate detective capabilities to be established and reported in a clear way. GuardDuty and CloudTrail are some services that can be parsed to have flags for specific malicious or noncompliant behavior. The attempts to access EC2 instances, uncredentialed and externally, is a clear auditable flag that can be identified and then dealt with. The primary concern, outside of secure and confidential business operations, is the access and compromise of secure payment information in storage. The use of explicit format matching for credit cards in this case, even tokenized, can raise alarms to this specific behavior. With this being a critical example, labeling and addressing the range of risk is integral to handling high priority

events/incidents first and possibly correlating even further. These aspects in mind, the time-spent on this must be relatively low, as responding and tracing the issue must occur as soon as possible.

Containment Phase:

In containing detected events, the pre-existing Zero-trust principles to configure implicit-denial to most services/users should limit cases of misconfiguration causing this. Containing in the context of S3 buckets or data processing can be done through policy specification that can be applied to restrict access. Furthermore, the preservation of logs and event monitoring will ensure that evidence is available for latter phases. Notifying relevant stakeholders through SNS, utilizing the sns.publish() function, can help automate the pipeline and reduce the latency in communication and actions. Outside of AWS CLI measures, the network-based issues/threats would be handled through AWS WAF, where specific agents, domains, or IP addresses can be blocked. This would prevent both ingress and egress traffic in the event of exfiltration or lateral movement.



Blocks to geolocations and specific addresses can be as follows above. The use of regular expressions within these access control lists and measures can provide a granular control over the pertaining threat actor/IoC (in the network perspective). These measures, may need to be custom if the aforementioned implicit-deny (for sensitive access) is not enough, but the general timeline of an hour for the response team to work through this should be enough. Especially with the monitoring and already stringent capabilities within Beetle Film's environment.

Eradication Phase:

With the threat identified and contained within the environment, the next phase involves the eradication of the associated threats. The efficacy of this phase is very reliant on the earlier phases, as leaving any remanence (pre or post-incident) still allows for compromise to affect operations. Worse yet, undiscovered footholds can still allow actors to fester and continue to damage the environment. The deprovisioning of resources must be done without damaging other systems/funcitonality as well, the IaC model for the organization allows for granularity and atomicity to catalyze this segmentation.

```
user = event['detail']['userIdentity']['userName']
keys = iam.list_access_keys(UserName=user)['AccessKeyMetadata']
for key in keys:
    iam.delete_access_key(UserName=user, AccessKeyId=key['AccessKeyId'])

secretsmanager = boto3.client('secretsmanager')
secretsmanager.rotate_secret(SecretId='compromised-db-creds')
```

Natively, compromised accounts being the main threat vector for this environment, account deprovisioning will be vital. Narrowing on user access-keys and revoking them can disable and remove account account for the time being. In general cases, this can be done through Lambda functions at scale, through AWS CLI scripts, or through the web interface. In rotating secrets, any possible compromise in keys can be revoked. API keys or other valuable secrets may also benefit from this, if hosted directly from AWS services, though external services may need connectivity reestablished. The malware proliferation (if applicable) may also be removed from servers/infrastructure through CLI, this may involve simply disabling and removing, but further measures must be taken if persistence is attempted to be established. In some cases, it may be easier to revert to a prior snapshot/version of systems if time is of importance. The design principles suggested for Beetle Films, stemming from *Task 2's Proposal,* ensure redundancy through deeper provisions as well as possible aid from AWS (in some extreme scenarios). The utilization of Terraform can allow for some improvements, depending on optimization and implementation.

Lastly, patching and remediating possible vulnerabilities within this phase is expected. In situations where patches for services are not readily available, mitigative measures may need to be provisioned or considered. Risk assessments may need to be retaken here to ensure that any further measures justify the risk handled. Though

this may be quite a lengthy process, the prior planning and ultization of playbooks (such as this one) can allow for speedy handling if not at least decision-making.

Recovery Phase:

This phase aims to restore downed systems, accounts, services, etc. to resume normal operations. The proper communication to stakeholders may be necessary beginning from this phase, though this is the sole focus of the *Communication Phase*. This may involve reprovisioning assets that were impacted. In the case of immutable servers/services, they may need to be reworked completely. The regular use of AWS Backup will allow for rolling services/systems to be restored from previous snapshots, reducing the concerns of downtime and availability considerably. The securing of BackupVaults through key rotation may also be necessary, pre and post-operation, to provide the highest level of security. The RTO for this procedure will usually be less than one day, though less-redundant and critical services in the future may stray from this metric.

Communication Phase:

Building from the outcomes of the *Recovery Phase* the necessary communication must be caried out to the associated stakeholders. Though internally the communication time may be relatively low, the upper-management/owners of Beetle Films will be reported to here. If inconclusive operations are carried out during the incident, then the upper-management can aid in providing further direction regarding funding and risk. Dependant on the criticality of the incident, users or external entities

may need to be informed, especially when concerning PCI adjacent incidents. Legal teams may also need to be kept aware for representative situations.

Overall, considering the worst, most-expansive case; communication to stakeholders internally must be as soon as possible, even in non-business hours. This will allow for holistic decision-making for the organization and for all risks and impacts to be considered. In most cases, Beetle Films should not be impacted to this extent as long as due care and due diligence are carried out (in the *Preparation Phase,* continually) and the IRP is followed.

Post-Incident Phase:

Following the end of incident-handling, the incident response procedure must be reviewed. Even if root-cause is not identified, an immediate debriefing can provide information and evidence later on. Performing a root-cause analysis, which may require a forensic investigation, can provide a definitive understanding of what caused disruption/compromise. The previously collected evidence and logs from CloudTrail and other mediums can be used to understand and timeline the event. The retrospective of communications during the incident can provide context and understanding.

With root-cause(s) identified, a final lessons-learned can be conducted summarizing and understanding all aspects of the incident. Most importantly, errors and necessary changes must be reflected on and noted. General process changes can be assimilated into this playbook or reinforced through tabletop simulations. Overall, the procedural and possibly administrative issues are aimed to be solved with this exercise.

References

Amazon. (2024). *AWS Pricing Calculator*. Calculator.aws. https://calculator.aws/#/addService

Amazon Web Services. (2013). *ISO/IEC 27001:2013 Compliance - Amazon Web Services (AWS)*. Amazon Web Services, Inc. https://aws.amazon.com/compliance/iso-27001-faqs/

Amazon Web Services. (2024). *Self-paced digital training on AWS - AWS Skill Builder*. Amazon Web Services, Inc. https://skillbuilder.aws/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2022). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

Github. (2019). *Pricing · Plans for every developer*. GitHub. https://github.com/pricing

Glassdoor. (2025, February). How much does an Aws Cloud Architect make? Glassdoor. https://www.glassdoor.com/Salaries/aws-cloud-architect-salary-SRCH_KO0,19.htm

Merritt, M, et al. (2024). *Building a Cybersecurity and Privacy Learning Program*. https://doi.org/10.6028/nist.sp.800-50r1

Mccallister, E., Grance, T., & Scarfone, K. (2010). *Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

NIST. (2023, October 16). *NIST Special Publication 800-63B*. Nist.gov; NIST. https://pages.nist.gov/800-63-3/sp800-63b.html

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations. Security and Privacy Controls for Information Systems and Organizations, 5(5). https://doi.org/10.6028/nist.sp.800-53r5

OWASP. (2018). *Serverless-Top-10-Project/OWASP-Top-10-Serverless-Interpretation-en.pdf at master · OWASP/Serverless-Top-10-Project*. GitHub. https://github.com/OWASP/Serverless-Top-10-Project/blob/master/OWASP-Top-10-Serverless-Interpretation-en.pdf

PCI Security Standards Council. (2018). PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1 For merchants and other entities involved in payment card processing. https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

PCI Security Standards Council. (2024). *Qualification & Training Programs for Implementing PCI Standards & Solutions*. (n.d.). Www.pcisecuritystandards.org. https://www.pcisecuritystandards.org/program_training_and_qualification/

Trusted Sec. (2025). *Services: PCI*. (2023). TrustedSec. https://trustedsec.com/services/pci