# 2 NEARA **Technical Infrastructure and Security Posture of Neara**

# **1. Executive Summary**

Neara is an Australian technology company that provides digital twin solutions specifically designed for the utilities sector. Their platform offers a sophisticated approach to network management, risk mitigation, and grid modernization by creating detailed 3D models of critical infrastructure. This report presents an analysis of Neara's technical infrastructure and security posture, drawing upon publicly available information. The findings indicate that Neara's platform is built upon a cloud-based Software as a Service (SaaS) architecture, leveraging advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) to deliver its analytical capabilities. The platform's foundation in "physics-enabled" modeling suggests a high degree of accuracy in simulating real-world scenarios for utility networks. Regarding security, Neara emphasizes data protection in its privacy policies, and its hiring practices suggest an awareness of and potential pursuit of industry-standard security certifications. However, a deeper understanding of the specific technical security controls in place requires further investigation. Overall, Neara demonstrates a commitment to providing a technologically advanced solution for the utilities industry, with a foundational awareness of security considerations.

**2. Neara's Technical Infrastructure: Foundation of the Digital Twin Platform**

* **2.1. Core Functionality: Building and Utilizing Digital Twins**  
  Neara's central offering revolves around a "physics-enabled" platform that constructs 3D interactive models of critical infrastructure networks and assets 1. This technology allows users to simulate a wide array of real-world events, enabling a comprehensive assessment of both current and potential future risks, such as those arising from adverse weather conditions or asset degradation 1. This capability extends to prioritizing maintenance schedules and formulating effective disaster response strategies. The term "physics-enabled" is noteworthy as it implies a sophisticated approach to modeling that likely integrates engineering principles and fundamental physical laws. This suggests that Neara's simulations are not merely visual representations but are grounded in a deeper understanding of how infrastructure behaves under various conditions, potentially leading to more accurate and reliable predictive capabilities.  
  The ability to simulate diverse scenarios represents a significant analytical advantage for utilities 4. By modeling potential impacts of events like major flooding, as experienced by Essential Energy during a pilot program, utilities can proactively plan and implement mitigation measures 4. This moves them away from a reactive operational stance towards a more predictive and preventative model, allowing for better resource allocation and reduced downtime. For instance, simulating the impact of severe weather allows utilities to identify vulnerable points in their network and test the effectiveness of potential remediation solutions before actual implementation 8. This proactive approach can lead to significant improvements in network resilience and reliability, ultimately benefiting both the utility and its customers.  
  Furthermore, Neara's platform caters to a broad spectrum of use cases within the utilities sector 4. These include ensuring network health and reliability by identifying and addressing risks faster, enhancing weather resilience and grid hardening by predicting and preparing for extreme weather, facilitating renewable energy and decarbonization efforts by optimizing existing network capacity, and improving emergency response through rapid flood analysis and power restoration 4. The versatility of the platform indicates a comprehensive solution designed to address the multifaceted challenges faced by modern utility companies as they navigate increasing demands, environmental pressures, and the transition to cleaner energy sources.
* **2.2. Underlying Technologies and Tools**  
  Neara's platform harnesses the power of Artificial Intelligence (AI) and Machine Learning (ML) to perform complex, engineering-grade analyses across the entire network infrastructure 1. The integration of AI and ML suggests advanced capabilities such as automated risk assessment, where the platform can analyze vast amounts of data to identify potential vulnerabilities without manual inspection 15. It also hints at predictive maintenance functionalities, allowing utilities to anticipate asset failures and schedule maintenance proactively, minimizing disruptions and costs 16. Additionally, AI/ML could be employed for anomaly detection, identifying unusual patterns in network behavior that might indicate potential issues or security threats.  
  The underlying technology stack comprises a range of programming languages and frameworks. Backend development utilizes languages such as Java, C++, and Python 17. These are robust and widely used languages known for their performance and scalability, suitable for handling the complex data processing requirements of Neara's platform. For the frontend, which provides the interactive 3D visualization of the infrastructure, Neara employs JavaScript/TypeScript, HTML, CSS, and WebGL 17. WebGL is particularly relevant as it enables high-performance rendering of 3D graphics within web browsers, crucial for visualizing intricate network models. User interface development leverages frameworks like React, Angular, or Vue 17. These modern JavaScript frameworks facilitate the creation of dynamic and responsive user experiences, essential for a platform that requires extensive user interaction with complex data.  
  Furthermore, Neara adopts Infrastructure as Code (IaC) practices, utilizing Pulumi for managing its infrastructure on Amazon Web Services (AWS) 18. Pulumi allows developers to define and deploy cloud infrastructure using familiar programming languages, enabling automation, version control, and repeatability in infrastructure management. This suggests a commitment to modern DevOps principles, leading to more efficient and reliable infrastructure deployment and maintenance. The combination of these technologies points towards a sophisticated, scalable, and highly interactive platform capable of processing large datasets, performing complex analyses, and providing users with rich, intuitive visualizations of their critical infrastructure.  
  **Table: Neara's Technology Stack Components**

| **Category** | **Specific Technology/Tool** | **Snippet ID(s)** | **Brief Description/Purpose** |
| --- | --- | --- | --- |
| Programming Languages | Java, C++, Python | 17 | Backend development for performance and scalability. |
| Frontend Technologies | JavaScript/TypeScript, HTML, CSS, WebGL | 17 | Interactive user interface and 3D visualization within web browsers. |
| Frameworks | React, Angular, Vue | 17 | Building dynamic and responsive user interfaces. |
| Infrastructure as Code | Pulumi | 18 | Automating the provisioning and management of cloud infrastructure on AWS. |
| AI/ML Technologies | AI, Machine Learning | 1 | Performing complex engineering analysis, risk assessment, and predictive modeling. |

* **2.3. Data Sources and Handling**  
  Neara's platform demonstrates the capability to process a diverse range of data sources, including LiDAR (Light Detection and Ranging) data, aerial photography, photogrammetry, and existing geospatial data in formats such as DXF, CSV, LAS, and KML 14. LiDAR technology, which uses lasers to create precise 3D maps of the environment, is particularly valuable for capturing detailed information about utility infrastructure and its surroundings 20. The ability to ingest and process these varied geospatial data formats highlights Neara's capacity to integrate with the existing data systems commonly used by utility companies. This allows them to leverage their existing investments in data collection and management to build accurate and comprehensive digital twins of their networks.  
  A key aspect of Neara's data handling is its capability to automatically process, clean, and extract valuable insights from raw LiDAR data at scale 4. Processing LiDAR data can be computationally intensive and time-consuming. Automation in this area suggests that Neara's platform is designed for efficiency and scalability, enabling utilities to rapidly generate and update their 3D models without relying on extensive manual processing. This efficiency is crucial for maintaining the accuracy and relevance of the digital twin, especially in dynamic environments where infrastructure or surrounding conditions may change frequently. The insights derived from this processed data can then be used for various applications, such as vegetation management, asset inspection, and risk assessment.
* **2.4. Cloud Infrastructure and Scalability**  
  Neara operates as a cloud-based enterprise SaaS platform 1. This deployment model offers significant advantages in terms of scalability, accessibility, and reduced operational overhead for its customers. As a SaaS solution, Neara manages the underlying infrastructure, software updates, and maintenance, allowing utility companies to focus on utilizing the digital twin capabilities without the need for significant in-house IT infrastructure or expertise to manage the platform itself.  
  Job descriptions for roles within Neara indicate that experience with both AWS and Google Cloud Platform (GCP) is valued 17. Furthermore, Neara's software offerings are available on the AWS Marketplace 2. The presence on the AWS Marketplace strongly suggests that AWS is a primary cloud provider for Neara. Leveraging AWS provides access to a vast array of scalable infrastructure and services, including computing power, storage, and networking, which are essential for supporting the performance and reliability demands of Neara's platform. The global reach of AWS also allows Neara to serve its international customer base effectively.  
  While AWS appears to be a key component of Neara's infrastructure, the mention of GCP in job descriptions could indicate a potential multi-cloud strategy. Adopting a multi-cloud approach can enhance resilience by reducing reliance on a single provider and offering greater flexibility in choosing services based on specific needs or cost considerations. It could also signify future plans for expanding their platform's availability to other cloud environments. Regardless of the specific cloud strategy, the cloud-based nature of Neara's platform is fundamental to its ability to scale and deliver its digital twin solutions to utility companies globally.

**3. Security Posture Analysis: Protecting Critical Infrastructure Data**

* **3.1. Privacy Policies and Data Handling Practices**  
  Neara has made its commitment to privacy evident through the publication of a privacy policy that outlines its practices for collecting, holding, using, and disclosing personal information 1. This policy details the various categories of personal information that Neara collects, which include standard contact information such as names, email addresses, phone numbers, and addresses, as well as technical information related to platform usage 1. This technical information encompasses IP addresses, login data, browser type, time zone settings, location data, and third-party access tokens. The collection of this type of information is typical for online platforms and serves purposes such as user authentication, security monitoring, and service improvement.  
  Within its privacy policy, Neara asserts that it has implemented appropriate security measures designed to prevent personal information from being accidentally lost, used, accessed without authorization, altered, or disclosed 1. Furthermore, the company states that it takes reasonable steps to protect personal information from misuse, interference, loss, unauthorized access, modification, or disclosure. This indicates a general awareness of the importance of data security. Additionally, Neara has established procedures to address any suspected personal information breaches, including protocols for notifying affected individuals and relevant regulatory bodies as required by law 1. While the privacy policy provides a foundational understanding of Neara's data handling principles, it lacks specific details regarding the concrete technical security controls and practices that underpin these commitments. A comprehensive assessment of their security posture would necessitate insights into the specific technologies and processes employed to safeguard sensitive data.
* **3.2. Security Certifications and Compliance Efforts**  
  An examination of Neara's hiring practices reveals a potential emphasis on security expertise and compliance with industry standards. A job description for a Senior Site Reliability Engineer (SRE) role explicitly states that security certifications and professional-level public cloud certifications, such as those from AWS and GCP, are highly desirable 26. Notably, this description also highlights the value of experience in guiding companies through ISO 27001 and SOC2 certifications. ISO 27001 is a globally recognized standard for information security management systems, providing a framework for establishing, implementing, maintaining, and continually improving an ISMS 32. SOC2 (System and Organization Controls 2) is an auditing procedure that ensures service providers securely manage data to protect the interests of their organization and the privacy of its clients, focusing on principles such as security, availability, processing integrity, confidentiality, and privacy 35.  
  The fact that Neara seeks candidates with experience in these specific certifications suggests that the company is either already certified in ISO 27001 and/or SOC2 or is actively pursuing these certifications. Obtaining these certifications demonstrates a strong commitment to adhering to established security best practices and provides assurance to customers, particularly those in regulated industries like utilities, that their data is being handled with appropriate security controls. The emphasis on public cloud certifications further underscores the importance of securing Neara's cloud-based infrastructure on platforms like AWS and potentially GCP. Cloud security requires specialized knowledge and skills, and seeking individuals with these certifications indicates a proactive approach to ensuring the security of their platform in the cloud environment.  
  **Table: Potential Security Certifications and Their Significance**

| **Certification Name** | **Brief Description of the Certification** | **Snippet ID(s) Indicating Neara's Interest/Mention** | **Significance for Utility Sector Clients** |
| --- | --- | --- | --- |
| ISO 27001 | International standard for information security management systems (ISMS). Provides a framework for managing and protecting information assets. | 26 | Demonstrates adherence to globally recognized security best practices. Often a requirement for enterprise clients and in regulated industries. |
| SOC2 | Auditing procedure ensuring service providers securely manage data based on trust service principles (security, availability, processing integrity, confidentiality, privacy). | 26 | Provides assurance about the security and reliability of the service provider's data management practices. Increasingly expected by businesses using SaaS providers. |

* **3.3. Access Controls, Authentication, and Authorization**  
  Within its privacy policy, Neara mentions the collection of "Neara usernames and passwords" as part of the technical information associated with user accounts 1. This indicates that a basic level of authentication, relying on username and password combinations, is in place for users to access the platform. While this is a standard method of authentication, the provided information does not detail the strength or sophistication of these mechanisms. For instance, it is unclear whether Neara employs multi-factor authentication (MFA), which adds an extra layer of security by requiring users to provide two or more verification factors to gain access. In the current cybersecurity landscape, especially when dealing with critical infrastructure data, the implementation of MFA is considered a crucial security control to mitigate the risks associated with compromised passwords.  
  Furthermore, the available information does not provide specific details regarding role-based access control (RBAC) or other authorization mechanisms within the Neara platform. RBAC is a method of restricting system access to authorized users based on their roles within the organization. Implementing RBAC ensures that users only have access to the data and functionalities necessary for their specific job responsibilities, reducing the risk of unauthorized actions or data breaches. Without information on these more granular access control measures, it is difficult to fully assess the security of data access within the Neara platform.
* **3.4. Incident Response and Data Breach Protocols**  
  Neara has stated in its privacy policy that it has established procedures to deal with any suspected personal information breaches 1. This includes the commitment to notify affected individuals and any applicable regulatory authorities in the event of a breach, as required by law. Having a well-defined incident response plan is a critical component of an organization's overall security preparedness. Such a plan outlines the steps to be taken in the event of a security incident, from initial detection and containment to eradication, recovery, and post-incident analysis. A robust incident response capability allows an organization to effectively manage and mitigate the impact of any security incidents, minimizing potential damage and ensuring a timely return to normal operations.  
  However, the provided snippets do not offer specific details about the intricacies of Neara's incident response protocols. Information such as the specific steps involved in incident detection, the procedures for containing and eradicating threats, the processes for data recovery, and the methods for conducting post-incident analysis to prevent future occurrences are not available. While the commitment to having such procedures in place is a positive indicator, understanding the specifics of these protocols would provide a more comprehensive view of Neara's ability to effectively respond to and recover from security incidents.
* **3.5. Security in the Context of Utilities Infrastructure and OT**  
  Neara's platform is specifically designed for the utilities sector, meaning it handles data related to critical infrastructure. This type of data is highly sensitive and often a prime target for cyberattacks due to the potential for significant disruption and impact on essential services 22. Securing digital twins of critical infrastructure presents unique challenges, particularly when considering the potential for integration with Operational Technology (OT) environments. OT systems control and monitor industrial operations, such as power generation and distribution, and have distinct security requirements compared to traditional Information Technology (IT) systems.  
  The provided research material does not explicitly discuss how Neara addresses the specific security challenges associated with OT environments within utilities. OT systems often involve legacy technologies with different communication protocols and security vulnerabilities than IT systems. If Neara's platform integrates or has the potential to integrate with these OT systems, it is crucial to understand the security measures in place to protect against potential threats that could impact the physical infrastructure. A comprehensive security strategy for a digital twin platform in the utilities sector should consider the unique aspects of both IT and OT security to ensure the safety, reliability, and resilience of the critical infrastructure being modeled.

**4. Potential Technical and Security Considerations for Digital Twins in Utilities**

* **4.1. Technical Challenges in Implementation and Maintenance**  
  Implementing and maintaining accurate digital twins of complex utility infrastructure presents several technical challenges. One significant hurdle is data complexity and quality 38. Utility networks generate vast amounts of data from various sources, and ensuring the accuracy, consistency, and timeliness of this data is crucial for the reliability of the digital twin. Inconsistencies or gaps in the data can lead to inaccurate simulations and potentially flawed decision-making based on the platform's analysis. Therefore, robust data governance frameworks and quality control measures are essential for Neara to ensure the integrity of its digital twin models.  
  Another challenge lies in the integration of the digital twin platform with the existing technology and systems used by utility companies 38. Utilities often have a mix of legacy systems and newer technologies, and ensuring seamless interoperability between Neara's platform and these diverse systems can be complex. This integration is vital for data exchange and for incorporating the digital twin into existing operational workflows. Careful planning and execution are required to overcome potential challenges related to different data formats, communication protocols, and system architectures.  
  Processing and analyzing real-time data from large-scale infrastructure networks demands a robust and scalable IT infrastructure 38. Digital twins are most valuable when they can provide up-to-date insights into the current state of the infrastructure. This requires the ability to efficiently process and analyze large volumes of data in near real-time. Neara's reliance on cloud infrastructure likely helps address this challenge by providing access to scalable computing and storage resources. However, optimizing data processing pipelines and ensuring low latency remain important considerations.  
  Finally, maintaining the long-term accuracy and relevance of the digital twin as the physical infrastructure evolves is an ongoing process 38. Utility networks are dynamic, with new assets being added, existing ones being upgraded or retired, and environmental conditions changing over time. The digital twin needs to be continuously updated to reflect these changes accurately. This requires established processes for data updates, model recalibration, and ongoing maintenance of the platform itself.
* **4.2. Cybersecurity Risks Associated with Digital Twins of Critical Infrastructure**  
  Digital twins of critical infrastructure, such as those provided by Neara, can become attractive targets for cyberattacks 22. The detailed information contained within these models about the configuration, status, and vulnerabilities of utility networks could be exploited by malicious actors. A successful cyberattack could potentially lead to data breaches, where sensitive information about the infrastructure falls into the wrong hands. Furthermore, attackers might attempt to manipulate the simulations within the digital twin, leading to incorrect analyses and potentially flawed operational decisions by the utility. In a worst-case scenario, if the digital twin platform has connections to OT systems that control the physical infrastructure, a cyberattack could even result in disruptions to essential services, posing significant risks to public safety and the economy.  
  Given these risks, ensuring the security of the cloud infrastructure hosting the digital twin is of paramount importance. Neara's reliance on AWS provides a foundation of security controls, as AWS invests heavily in securing its global infrastructure. However, Neara also has a responsibility to implement its own security measures on top of this foundation, such as configuring access controls, managing security updates, and monitoring for suspicious activity. Protecting the integrity and confidentiality of the data used to build and operate the digital twin is also crucial. This includes implementing strong data encryption mechanisms, both when the data is stored (at rest) and when it is being transmitted (in transit). Encryption helps to prevent unauthorized access to sensitive information, even if a breach were to occur.
* **4.3. Recommendations for Enhancing Technical Infrastructure Resilience and Security Posture**  
  Based on the analysis of the available information, several recommendations can be made to further enhance Neara's technical infrastructure resilience and security posture:
  + Implement multi-factor authentication (MFA) for all user accounts accessing the platform. This adds a critical layer of security beyond just usernames and passwords.
  + Provide greater transparency regarding the specific security controls and certifications that Neara has implemented or achieved. Publishing security whitepapers or audit reports could help build trust with potential clients.
  + Offer more detailed information about the incident response plan and data breach notification procedures to assure clients of their preparedness in case of a security incident.
  + If the platform integrates or has the potential to integrate with OT systems, clearly outline the security considerations and measures in place to protect these critical environments.
  + Establish a continuous security monitoring and update program to proactively address emerging threats and vulnerabilities. Regular security assessments and patching are essential.
  + Consider engaging independent third-party security firms to conduct regular security audits and penetration testing of the platform to identify and address any potential weaknesses.
  + Implement robust data validation and quality checks throughout the data ingestion and processing pipelines to ensure the accuracy and reliability of the digital twin models.
  + Develop and maintain a comprehensive data backup and recovery strategy to ensure business continuity in the event of a system failure or disaster.

**5. Conclusion**

Neara presents a technologically advanced platform for the utilities sector, leveraging a cloud-based architecture and sophisticated technologies like AI/ML to create "physics-enabled" digital twins of critical infrastructure. This approach offers significant potential for utilities to enhance network management, mitigate risks, and modernize their operations. The platform's ability to handle diverse geospatial data and perform complex simulations underscores its technical capabilities. Regarding security, Neara demonstrates a foundational awareness of data protection through its privacy policies, and its hiring practices suggest a commitment to industry-standard security certifications. However, more granular details regarding specific technical security controls and incident response protocols are needed for a comprehensive security posture assessment. Given the sensitivity of utility infrastructure data and the potential risks associated with cyberattacks on critical infrastructure, maintaining a strong and transparent security posture is paramount for Neara's continued success and the trust of its clients.

#### Works cited

1. About Us - Neara, accessed March 19, 2025, <https://neara.com/about/>
2. Neara Software - AWS Marketplace, accessed March 19, 2025, <https://aws.amazon.com/marketplace/seller-profile?id=6e675b22-a187-476b-8217-96e746717a27>
3. Neara - Matchstiq, accessed March 19, 2025, <https://matchstiq.io/companies/Neara>
4. Electric Utility Software | Neara, accessed March 19, 2025, <https://neara.com/home/>
5. Flood Analysis and Emergency Response | Neara, accessed March 19, 2025, <https://neara.com/flood-analysis-and-emergency-response/>
6. Why Neara, accessed March 19, 2025, <https://neara.com/why-neara/>
7. Neara: Overview, accessed March 19, 2025, <https://neara.com/neara-overview/>
8. Neara: Electric Utility Software, accessed March 19, 2025, <https://neara.com/>
9. AWS Marketplace: Design, Analyze and Spatial Modules, accessed March 19, 2025, <https://aws.amazon.com/marketplace/pp/prodview-mlbmlvn67d666>
10. How To Fix The Greatest Threat to Reliability and Resilience | Neara, accessed March 19, 2025, <https://neara.com/digital-reliability-risk-mitigation-primer/>
11. Green Energy Transition for Utilities with Neara, accessed March 19, 2025, <https://neara.com/green-energy-transition-for-utilities-with-neara/>
12. AI power grid modeling platform Neara raises $31 million - Factor This™, accessed March 19, 2025, <https://www.renewableenergyworld.com/power-grid/smart-grids/ai-power-grid-modeling-platform-neara-raises-31-million/>
13. Renewable Energy & Decarbonization - Neara, accessed March 19, 2025, <https://neara.com/renewable-energy-decarbonization/>
14. Weather Resilience & Grid Hardening | Neara, accessed March 19, 2025, <https://neara.com/weather-resilience-grid-hardening/>
15. Neara's AI Solutions: Safeguarding Utilities Against Extreme Weather - Multiplatform AI, accessed March 19, 2025, <https://multiplatform.ai/nearas-ai-solutions-safeguarding-utilities-against-extreme-weather/>
16. How Digital Twins Can Solve Your Facility Management Challenges | Matterport, accessed March 19, 2025, <https://matterport.com/ko/blog/digital-twin-facility-management>
17. Senior Full Stack Software Engineer - linq, accessed March 19, 2025, <https://app.linq.co/en/job/9526>
18. Neara-Software/simple\_lambda\_test - GitHub, accessed March 19, 2025, <https://github.com/Neara-Software/simple_lambda_test>
19. Overhead and Underground Network Design | Neara, accessed March 19, 2025, <https://neara.com/overhead-and-underground-network-design/>
20. LiDAR Utilization for Utilities - Neara, accessed March 19, 2025, <https://neara.com/lidar-utilization-for-utilities/>
21. Network Digitization - Neara, accessed March 19, 2025, <https://neara.com/network-digitization/>
22. The Competitive Landscape of Neara - CANVAS, SWOT, PESTEL & BCG Matrix Editable Templates for Startups, accessed March 19, 2025, <https://canvasbusinessmodel.com/blogs/competitors/neara-competitive-landscape>
23. Neara - Kula, accessed March 19, 2025, <https://careers.kula.ai/neara>
24. Neara Marketing Mix Analysis – CBM, accessed March 19, 2025, <https://canvasbusinessmodel.com/products/neara-marketing-mix>
25. Neara | EU-Startups, accessed March 19, 2025, <https://www.eu-startups.com/directory/neara/>
26. Neara - Kula, accessed March 19, 2025, <https://careers.kula.ai/neara/321>
27. Learn More - Neara, accessed March 19, 2025, <https://neara.com/learn-more/>
28. Clearance Analysis | Neara, accessed March 19, 2025, <https://neara.com/clearance-analysis/>
29. New Careers Page | Neara, accessed March 19, 2025, <https://neara.com/about/careers-at-neara/>
30. Neara Privacy Policy, accessed March 19, 2025, <https://neara.com/privacy-policy/>
31. Candidate Privacy Policy - Neara, accessed March 19, 2025, <https://neara.com/candidate-privacy-policy/>
32. Nearsure Attains the ISO 27001 Certification –and Here's How You Can Get Yours, too, accessed March 19, 2025, <https://www.nearsure.com/blog/nearsure-attains-the-iso-27001-certification>
33. ISO 27001 Certification - Information Security System - NQA, accessed March 19, 2025, <https://www.nqa.com/en-us/certification/standards/iso-27001>
34. ISO 27001 Certification Process: A Step-by-Step Guide | Secureframe, accessed March 19, 2025, <https://secureframe.com/hub/iso-27001/certification-process>
35. Why SOC 2 Certification is the New Standard for Security in Research Administration, accessed March 19, 2025, <https://cayuse.com/blog/soc-2-certification-research-administration-security/>
36. What is SOC 2 | Guide to SOC 2 Compliance & Certification - Imperva, accessed March 19, 2025, <https://www.imperva.com/learn/data-security/soc-2-compliance/>
37. System and Organization Controls (SOC) 2 Reporting (SOC 2 Report) - LogRhythm Documentation, accessed March 19, 2025, <https://docs.logrhythm.com/kbmodules/docs/system-and-organization-controls-soc-2-reporting-s>
38. Digital Twin Implementation - Challenges & Practices - Toobler, accessed March 19, 2025, <https://www.toobler.com/blog/challenges-in-digital-twin-implementation>