DDN1 Task 2: Project Proposal

Cyber Security Graduate Capstone – D490

John Luong

Western Governors University

A1. Importance of the Security Problem

The security problem under investigation at Jotoan Financial Services (JFS) is the lack of a unified, scalable, and resilient security model to protect its future hybrid infrastructure. As JFS makes its transitions to a hybrid cloud environment, retaining the company's on-premises systems while simultaneously migrating its critical workloads to Microsoft Azure creates an increase in complexity in safeguarding digital assets across both environments.

JFS currently relies on a traditional perimeter-based security model and fragmented access controls, which do not hold effectively against modern and possible new threats that includes credential theft, ransomware, and lateral movement within networks. Moving towards this hybrid environment also creates security gaps, specifically with over-permissioned legacy accounts in Active Directory, inconsistencies in identity management, incomplete deployment of multifactor authentication, and minimal visibility in lateral network movements.

Jotoan's current tool for hybrid identity synchronization; Active Directory Federation Services (ADFS), further complicates enforcement of Conditional Access and dynamic-risk based policies. These weaknesses contradict Zero Trust Principles such as "never trust, always verify" and "assume breach," which are essential when securing modern enterprise infrastructures (NIST, 2020; CISA, 2023). As supported by frameworks like NIST SP 800-207 and CISA's Zero Trust Maturity Model v2.0, transitioning to a Zero Trust Architecture (ZTA) is a necessity to protect and fortify JFS's assets against evolving cyber threats.

A2. Documentation Demonstrating the Need for a Solution

The proposed solution is necessary by the supporting evidence from several reputable industry and government sources, such as NIST SP 800-207, since Zero Trust Architecture outlines the foundational principles of a Zero Trust Architecture and emphasizes continuous identity validation, real-time policy enforcement, and least privilege access which directly falls in line with JFS's identified security challenges (NIST, 2020). Next is the CISA Zero Trust Maturity Model v2.0 which has a structured roadmap for adopting Zero Trust with identifying common obstacles such as legacy authentication systems and lack of identity visibility that JFS currently faces (CISA, 2023). Furthermore, Microsoft explicitly states that Active Directory Federation Services, while supporting hybrid identity, lacks the native policy granularity of Azure Active Directory (Azure AD), limiting Conditional Access enforcement in cloud environments (Microsoft 2023). In addition, MITRE ATT&CK Framework contains documented attack patterns involving lateral movement and credential abuse which are key vulnerabilities currently unmonitored within JFS's infrastructure (MITRE, 2023). Likewise, CrowdStrike advocates for a Zero Trust model that prioritizes identity, endpoint visibility, and behavioral analytics (CrowdStrike, 2023). Palo Alto Networks provides a roadmap for the implementation of Zero Trust across identity, applications, and infrastructure that emphasizes the practice of continuous validation and device context (Palo, 2023). Google's Beyond Corp framework demonstrates a working Zero Trust model that replaces perimeter trust with a solid, identity-aware access controls and endpoint compliance verification (Google, 2020). Overall, these sources provide justification for implementing Zero Trust at Jotoan Financial Services and demonstrate how current modern frameworks and tools can directly resolve the company's most pressing security issues.

A3. Root Causes of the Security Problem

JFS's security vulnerabilities stem from several underlying root causes starting with outdated security architecture; JFS's perimeter-based model assumes there's internal network trust, which is ineffective in a hybrid cloud environment where users and services operate outside of their typical boundaries. Another is its legacy identity infrastructure because JFS being reliant on ADFS as well as a fragmented identity and access management (IAM) strategy leads to excessive privilege assignments, minimal role governance, and gaps in support for real-time access decisions. Moreover, the company's inconsistent multi-factor authentication (MFA) and Conditional Access causes many users and systems to lack MFA with ADFS which leads to poor support for dynamic, risk-based policies thus leaving JFS vulnerable to credentialed attacks. On top of that, having no centralized logging and threat analysis tools, like Microsoft Sentinel and Microsoft Defender for Identity, hinders real-time detection of threats such as lateral movement or insider attacks which brings weak unified monitoring and detection. In the same vein, it has a disjointed policy enforcement within its hybrid environment because it lacks a centralized control plane. This inevitably created gaps that adversaries can exploit since there's no enforcement of access policies across on-premises and the cloud. Ultimately, addressing these root causes through a Zero Trust implementation will provide JFS with a structured, scalable, and standards-compliant security framework specifically tailored to its hybrid infrastructure.

B: Stakeholder Summary

The implementation of the Zero Trust Architecture (ZTA) roadmap at Jotoan Financial Services (JFS) involved a diverse set of internal and external stakeholders, each playing a critical role in the project's direction, execution, and successful outcomes.

The chief information security officer (CISO) serves as the executive sponsor that's responsible for overseeing the company's overall cybersecurity strategy. The CISO's role is centered on ensuring the project aligns with JFS's risk management goals and compliance obligations. The company's security gaps, such as giving over permissions for legacy systems and lack of policy enforcement, exposes them to regulatory risk and reputational harm. Thus, the CISO strongly influenced the project's strategic objectives and ensured governance standards were met throughout.

The chief information officer (CIO) is responsible for aligning the ZTA implementation with JFS's overall digital transformation strategy. Since the organization transitioned to Microsoft Azure while maintaining on-premises systems, the CIO ensured that the integration of security controls did not disrupt business continuity. With the fragments in identity infrastructure and legacy tools, it directly impacts the CIO's ability to modernize IT services. Therefore, the CIO's influence helped prioritize the phased rollout and allocated resources to ensure operational stability.

IT operators played a pivotal role during the configuration and simulation phases of the project. They were tasked with maintaining the existing active directory environment and ensuring compatibility with Azure Active Directory (Azure AD) and Active Directory Federation

Services (ADFS). The outdated access control mechanisms in the company created unnecessary complexities in their daily operations. Subsequently, the IT operators' input played a major role in identifying legacy dependencies and implementing changes without introducing service interruptions.

The security team took charge in deploying Microsoft Sentinel and Defender for Identity. Their involvement included configuring detection rules, monitoring telemetry, and validating threat analytics within the hybrid infrastructure. Previously, JFS lacked centralized logging and visibility which hindered their ability to detect lateral movements and insider threats. With the team's success, they were able to directly shape the effectiveness of threat detection capabilities and the refinement of identity-based policies.

The compliance officers ensured that the security controls designed and implemented throughout the project supported JFS's legal and regulatory requirements. Earlier beforehand, the company did not have consistent access control and audit readiness which poses a significant risk to regulatory compliance. To deter any fines and legal problems, compliance officers reviewed documentation, configurations, and assessments reports to confirm adherence to standards such as NIST SP 800-207 and CISA's Zero Trust Maturity Model (NIST, 2020; CISA, 2023). Their constant validation throughout the whole duration of the project was key to defining audit-ready processes and supporting long term governance.

Internal users, including general employees, were indirectly involved through user acceptance testing and change management feedback. Prior to implementation, there was insufficient MFA coverage and poor access visibility that left users exposed to possible phishing, credential theft, or session hijacking. With their input and feedback during the testing phases, internal users played an influence in policy adjustments. Internal users, especially those related

to Conditional Access and user experience, ensured the new security controls were both secure and practical.

Application owners engaged in the project to assess the impact of the new identity controls on legacy and cloud-based applications. Since JFS relied on consistent authentication mechanisms, application owners validated integration with Azure AD and Conditional Access policies. The hybrid security gap had left vulnerabilities in application functionality and availability, but application owners were able to coordinate and help ensure a seamless user experience while maintaining secure access.

Lastly, cloud architects were essential in designing and redefining the Azure-based infrastructure to support Zero Trust principles. In the past, their work was limited due to the limited visibility and policy enforcement capabilities of ADFS. Over the course of the project, they led the development of access controls, identity governance structures, and scalable cloud integrations that will support both current and future infrastructure needs. They were able to ensure that the Zero Trust roadmap was secure, architecturally sound, and scalable.

Altogether, these stakeholders contributed to a collaborative, structured implementation of Zero Trust that has strengthened JFS's security posture, reduced its attack surface, and aligned security operations with national frameworks and modern cloud environments.

C. Historical Data Used to Support Decision Making

Throughout the Zero Trust Architecture (ZTA) project at Jotoan Financial Services (JFS), several sources of historical data were utilized to guide security decisions and prioritized implementation phases. The data used provided insight into the organization's vulnerabilities, system dependencies, and overall security maturity which all provided information to design the roadmap and align the project with industry best practices.

The most influential data sources came from internal security assessments and Active Directory audits that were conducted prior to the project. These audits revealed critical level issues such as over-permissioned legacy accounts, a lack of role-based access controls, and inconsistencies of multi-factor authentication (MFA). And based off the data, it directly influenced the project's early focus on identity and access hardening, including the integration of Azure Active Directory, the simulation of Conditional Access, and privileged identity management (PIM).

In addition, there's evidence of limited policy enforcement and revealed challenges in tracking authentication requests across hybrid systems from audit logs and system monitoring reports from existing Active Directory Federation Services (ADFS). This justified the shift toward Azure AD's cloud-native access control mechanisms, which allowed for a more granular, risk-based decision making.

Vulnerability scan reports from JFS's endpoint and network-level tools were also referenced to identify unpatched systems and insecure configurations that were susceptible to lateral movements and credential-based attacks. The findings from the reports were mapped to tactics and techniques based on the MITRE ATT&CK framework that allowed the security team

to simulate specific attack scenarios during the implementation of Microsoft Sentinel and Microsoft Defender for identity (MITRE, 2023). These tools were selected because it had the ability to close detection gaps that were discovered in past incident logs and help mitigate previously undetected behaviors in the legacy network.

JFS also referenced compliance audit results that are related to HIPAA and PCI-DSS, which flagged for inconsistencies in access control documentation, lack of centralized policy management, and insufficient evidence of continuous monitoring. This highlighted the necessity for a Zero Trust model that could demonstrate traceable, real-time policy enforcement across all systems. As a result, the gaps in compliance from the company became critical drivers behind the roadmap's governance and reporting objectives.

Finally, input from user access reviews and internal IT service desk tickets indicated recurring issues with account provisioning, password resets, and unauthorized access attempts. This type of data from the company helped further emphasize the need for identity modernization and secure onboarding workflows.

In combination, the historical data presented provides a clear justification for each phase of the ZTA roadmap, starting from identity hardening and threat detection to compliance readiness and policy governance. Leveraging the data mentioned enables a risk-informed, evidence-based approach that ensured the solution addresses strategic goals and points of operational inefficiencies within JFS's hybrid environment.

D1. Industry Standard Methodologies Guiding the Solution's Design and Development

The project's design and development for the solution were guided by two primary industry standard frameworks: NIST SP 800-207 Zero Trust Architecture and CISA Zero Trust Maturity Model v2.0 (NIST, 2020; CISA 2023). Both frameworks were instrumental in defining the principles, security layers, and maturity targets needed to successfully carry out Zero Trust in a hybrid environment.

NIST SP 800-207 framework provided foundational guidance on principles such as least privilege, continuous authentication, and explicit verification (NIST, 2020). This defined the architectural components of a Zero Trust system that helped the team build a solution that emphasized user identity, device health, policy enforcement, and robust logging. The CISA Zero Trust Maturity Model v2.0 offers a phased maturity model to assess Jotoan Financial Services' current capabilities, identify security gaps, and set realistic phased improvement targets across five key pillars; Identity, Device, Network/Environment, Application Workload, and Data (CISA, 2023).

In addition to these frameworks, Microsoft's Zero Trust guidance played a helpful role in aligning the solution with cloud-native technologies such as Azure Active Directory, Conditional Access, Microsoft Sentinel, and Microsoft Defender for Identity (Microsoft, 2023). These tools were chosen for their technical capabilities, but more so for their alignment with security best practices outlined by trusted vendors and security standards organizations.

Leading publications from CrowdStrike, Palo Alto Networks, and Google's BeyondCorp model influenced JFS's implementation pattern and its threat-centric design strategies that

supported the strength of endpoint controls, continuous authentication, and identity-driven enforcement (CrowdStrike, 2023; Palo Alto, 2023; Google, 2020).

D2. Project Launch, Rollout Phases, Completion Criteria, and Project Management Methodology

The project was executed over a simulated eight-week timeframe using the Agile project management methodology. This approach supported continuous improvement and stakeholder collaboration through four distinct phases of Zero Trust implementation.

First phase is Discover and Assessment (weeks 1-2) in which the team conducted a comprehensive inventory of existing identity and access control configurations within the company. They also evaluated JFS's Zero Trust maturity using the CISA's model and identified all legacy systems that were still dependent on ADFS.

The second phase, Identity and Access Hardening (weeks 3-4), focused on strengthening identity governance by configuring Azure Active Directory, enabling Conditional Access, enforcing MFA policies, and simulating PIM for elevated accounts. While in this phase, ADFS was maintained to preserve compatibility with legacy systems while transitioning toward a more robust, cloud-native access controls.

In the third phase, Monitoring and Threat Detection (weeks 5-6), the team deployed Microsoft Sentinel to centralize security logging and analytics as well as integrated Microsoft Defender for Identity to enhance threat visibility and detect suspicious lateral movements. JFS simulated attack scenarios based on the MITRE ATT&CK framework which were executed within the hybrid environment to validate the detection and response capabilities (MITRE, 2023).

The final phase, Roadmap and Governance (weeks 7-8), involves drafting a comprehensive implementation roadmap that's tailored towards JFS's environment. Additionally, it includes a proposed long-term strategy to eventually decommission ADFS and the development of a governance plan aligned with NIST SP 800-207 and the CISA Zero Trust Maturity Model.

The project was deemed complete once all major Zero Trust components, such as MFA, Conditional Access, PIM, Microsoft Sentinel, and Microsoft Defender for Identity; were configured and successfully simulated. Total completion criteria also required the fulfillment of decommissioning ADFS with supporting documentation including architectural diagrams, policy templates, and maturity assessments. Regular sprint reviews and stakeholder feedback loops ensured that each deliverable was aligned with JFS's technical requirements and business objectives. All under the estimation that the project that started on May 28th, 2025; would be fully completed around July 28th, 2025.

D3. Implementation Risks and Their Likelihood and Impact

Several risks were identified during the planning and execution of the project, each carrying different levels of likelihood and potential impact on outcomes. One significant risk was the legacy system compatibility, which was a moderate likelihood of occurring but with high impact. Many JFS's older applications and services relied on ADFS for authentication thus transitioning to Azure AD introduced compatibility concerns for legacy systems. To mitigate this, ADFS was temporarily retained during the project while cloud-native integrations were tested,

reducing the risk of authentication failures or service disruptions. Moreover, a decommissioning roadmap was developed for long-term removal of ADFS, pending legacy system migration.

Another concern was policy misconfiguration, which also had moderate likelihood and moderate impact. Potential errors in configuring Conditional Access or PIM could have resulted in unintentionally blocking legitimate user access or failure to properly enforce least privilege controls. This was mitigated by incorporating iterative testing into each sprint and using simulated user scenarios to validate access configurations before implementation.

There was also the consideration of limited user adoption or pushback, especially in response to the new MFA requirements or stricter access policies. Even though the likelihood was low, the potential for moderate impact on user productivity or satisfaction was enough to address it as a necessity to fix. This was effectively managed through proactive communication, user testing, and incorporating employee feedback to adjust the policies.

Monitoring gaps or tool misalignment was another risk that had a low likelihood but a high potential impact. Integration errors or misconfigured SIEM rules would have led to certain threats undergo undetected. To address this, the team utilized Microsoft Sentinel with simulations based on the MITRE ATT&CK framework to validate and optimize threat visibility across JFS's hybrid environment.

Lastly, the risks of insufficient governance or documentation carries a high long-term impact even though it was a low likelihood of occurring. Without proper documentation and policy governance, JFS would have faced challenges in sustaining security posture or demonstrating compliance in future audits. Prevention of this was planned in the final phase of

the project which emphasized the development of governance templates, detailed roadmap documentation, and policy lifecycle planning.

By addressing these risks through Agile feedback loops, stakeholder engagements, and structured validation processes, the project maintained strong alignment with its objectives and ultimately delivered a scalable and secure Zero Trust roadmap tailored to JFS's hybrid cloud infrastructure.

E. Training Approach

The training approach for the ZTA implementation at JFS was designed to ensure that adoption, security awareness, and operational readiness across all key stakeholder groups (NIST, 2020; CISA, 2023). The training effort supported the overall goal of operationalizing identity-based security, enforcing access controls, and ensuring long-term sustainability of the Zero Trust model.

The audience in training was separated into three primary groups: internal users (general employees), technical personnel (IT operators, security teams, application owners), and executive stakeholders (CIO, CISO, compliance officers). Each group received training that was tailored to their role and the level of involvement with the new security framework.

Delivery methods caried to suit each audience's needs. For internal users, training was delivered through interactive webinars and recorded instructional videos that focused on how to navigate through the new authentication processes including MFA enrollment and Conditional Access prompts. These training sessions were accompanied by job aids and quick-reference guides. For the technical teams, training was hands-on workshops that were conducted via live

virtual labs where IT and security staff configured, monitored, and validated the components of the new ZTA solution (e.g., Azure AD policies, Microsoft Sentinel alerts, and Microsoft Defender for Identity rules). Executive stakeholders received focused briefings that highlighted the strategic governance responsibilities, policy lifecycle management, and compliance reporting expectations.

In terms of content for the training, it was aligned with each group's operational needs. End-user content focused on usability, secure login behavior, and device compliance practices. Technical content covered identity integration, Conditional Access policy tuning, log analysis, and security incident response workflows. Executive content emphasizes Zero Trust governance, risk reduction metrics, and the alignment with NIST SP 800-207 and the CISA Zero Trust Maturity Model (NIST, 2020; CISA, 2023).

The total duration of the training initiative spanned around two weeks. Internal user sessions were typically around 30 to 45 minutes with optional follow-up Q&A opportunities. Technical workshops lasted around 1.5 to 2 hours per session and held across multiple business days to allow deep dives into each solution component. Executive briefings were conducted in 1-hour sessions with accompanying policy and roadmap documentation for review.

All things considered, the training approach ensured that all relevant stakeholders were prepared to operate in the new Zero Trust model and successfully handle its adoption across their respective teams. This structured and role-based training strategy was strongly impactful for enabling a smooth transition, minimizing disruption, and embedding security into Jotoan Financial Services.

F. Required Resources and Cost Sourcing

The success of the ZTA implementation at JFS required a combination of technical tools, personnel, and training resources during all project phases. Resources were planned and allocated based on tasks/objectives of each phase, with cost estimates sourced from publicly available documentation from Microsoft, MITRE, and other vendors.

Phase 1 (Discovery and Assessment), internal IT operators, cloud architects, and security analysts conducted security posture evaluations and inventory assessments. No new tools were purchased, thus only labor costs were accounted for which estimated at $60/hour over 20 hours per person, totaling around $7,200.

In phase 2 (Identity and Access Hardening) required Microsoft 365 E5 Security licenses to support Azure AD, MFA, Conditional Access, and PIM features. Their licensing is priced at $12/user/month for 1,000 users, so the total for a 3-month simulation was approximately $36,000. Labor for setup and testing added to an estimated $9,000 at $75/hour.

Phase 3 (Monitoring and Threat Detection) included deploying Microsoft Sentinel and Defender for Identity. Microsoft Sentinel's estimated monthly cost for 100GB/day was $730, and Microsoft Defender for Identity was $3,000/month. Security analysts worked 40 hours per week at $80/hour, totaling $12,800. MITRE ATT&CK simulations were conducted by utilizing free public tools online.

Lastly, phase 4 (Roadmap and Governance) involved project managers and compliance officers that producing documentation and governance materials. Estimated labor costs were at $85/hour for 60 hours which totaled around $5,100. Documentation software was already covered under existing Office 365 licenses at JFS.

Resource / Activity	Estimated Cost	Source
Security Analyst (Phase 1)	$7,200	JFS company estimate
Microsoft 365 E5 Security (3 mo, 1000 users)	$36,000	Microsoft (2023)
Technical Labor (Phase 2)	$9,000	JFS Company estimate
Microsoft Sentinel (100GB/day	$730/month	Microsoft (2023)
Microsoft Defender for Identity	$3000/month	Microsoft (2023)
Security Analyst Labor (Phase 3)	$12,800	JFS Company estimate
Governance Labor (Phase 4)	$5,100	JFS Company estimate
MITRE ATT&CK Framework	Free	MITRE (2023)
Microsoft Office Tools	Existing License	JFS
Total (approximate, 3-month window)	$74,830	

G. Project Deliverables and Timeline

The deliverables for the final project from the ZTA implementation at JFS ensured a comprehensive, actionable, and standards-aligned strategy for long-term cybersecurity enhancement. The deliverables included a detailed Zero Trust implementation roadmap, a phased plan for the decommissioning of ADFS, identity and access control policy templates (including those for MFA), Conditional Access, and PIM as well as an enterprise governance framework. Additional documentation included architectural network diagrams, Microsoft Sentinel alert configurations, MITRE ATT&CK-based simulation results, and CISA-aligned maturity assessment reports. All materials were compiled together using Microsoft Word and Visio to present to each team respectively (executive, compliance, technical). These deliverables

functioned as reference materials for operational execution and as documentation for compliance and strategic oversight.

The project simulated an eight-week Agile methodology timeline with key milestones and deliverables produced in bi-weekly sprints. The project began on May 28th, 2025, and concluded on July 28th, 2025. The first sprint (weeks 1-2) in which the team completed the discovery and assessment phase within the company. This consisted of a full Zero Trust maturity evaluation using CISA's Zero Trust Maturity Model v2.0 along with the company's inventory of current IAM infrastructure and the assessment of ADFS dependencies. During this first sprint, security analysts, IT operators, and cloud architects were the primary individuals for these tasks.

The second sprint (weeks 3-4) focused on identity and access hardening which included the configuration and simulation of Azure AD, enforcement of MFA policies, application of Conditional Access rules, and implementation of PIM. Azure engineers, security administrators, and IAM specialists led the technical execution of this sprint.

Sprint three (weeks 5-6), put their efforts towards monitoring and threat detection. This sprint consisted of deploying Microsoft Sentinel for centralized security logging and integrating Microsoft Defender for Identity to provide lateral movement detection and insider threat monitoring. Security engineers, SOC analysts, and Microsoft Sentinel administrators conducted simulations using the MITRE ATT&CK framework to validate threat detection effectiveness.

The fourth and final sprint (weeks 7-8) was dedicated to roadmap finalization and governance documentation. This phase resulted in the delivery of the completed Zero Trust roadmap, the decommissioning plan of ADFS, a governance strategy aligned with NIST and CISA frameworks, and supporting documentation including executive summaries and policy

lifecycle planning. The core team for this phase included the project manager, compliance officers, cloud architects, and technical writers.

Across all phases, planning, execution, validation, and stakeholder review were continuously integrated through Agile ceremonies. Total resource efforts across all sprints was approximately 240 to 300 hours, allocated among technical, compliance, executive, and operational stakeholders. This structured phased approach ensured that all deliverables were relevant, technically sound, and aligns with organizational and industrywide cybersecurity goals.

H. Project Evaluation Approach

The project evaluation strategy for the ZTA implementation at JFS conducted both formative and summative testing to assess the functionality, effectiveness, and alignment of the solution with cybersecurity goals. This dual approach ensured continuous improvement during implementation and a comprehensive final assessment success.

Formative testing was performed throughout each sprint cycle that included simulation-based configuration reviews, policy validation, and access control testing using predefined cases. Tools such as Azure AD sign-in logs, Conditional Access testing environments, and Microsoft Defender for Identity reports (Microsoft, 2023) were used to validate policy application and identity detection capabilities. Microsoft Sentinel dashboards (Microsoft, 2023) were also evaluated during testing to ensure that systems were collecting logs correctly and connecting related events properly. Test cases included to verify users logging in with or without MFA, risk-based access scenarios, lateral movement simulations using MITRE ATT&CK patterns, and endpoint compliance checks (MITRE, 2023; Microsoft, 2023). This phase was primarily

executed by security analysts and IT engineers, who provided feedback at the end of the sprint for adjustments.

Summative testing was conducted during the final project sprint and focused on end-to-end validation of all security controls and monitoring capabilities. This included complete run throughs of identity lifecycle events (e.g., offboarding, onboarding, access elevation), validation of alert response time in Microsoft Sentinel, and review of policy enforcement logs across Azure AD and Microsoft Defender for Identity. These tests were designed to emulate real world access and threat scenarios as well as measure system behavior under predefined conditions. The test tools used included Microsoft Sentinel's analytics rule reports, Azure AD sign-in logs, and the CISA Zero Trust Maturity Model rubric to reassess organizational alignment with Zero Trust principles.

Minimal acceptance criteria for the project included the successful enforcement of MFA for all non-privileged users, Conditional Access rules for at least two device posture conditions, accurate alerting of lateral movement attempts, and operational readiness of the Zero Trust roadmap with stakeholder approval. Key performance indicators (KPIs) for acceptance included reduction in open IAM audit findings, policy accuracy rate above at least 95%, Microsoft Sentinel alert correlation within five minutes of event ingestion, and full CISA maturity model scoring progress from "Traditional" to "Intermediate" across at least three pillars. These KPIs ensured that the system was functional, measurable, and ready for future operational rollouts.

Test cases and scenarios were justified based on the hybrid environment's security risks, especially concernment over-permissioned accounts, lateral threat movements, and fragmented access controls. Testing PIM, MFA coverage, and Microsoft Sentinel's real-time analytics capabilities directly addressed these issues. Additionally, test scenarios were aligned with known

attack patterns from MITRE ATT&CK to ensure detection mechanisms were robust against common attack vectors.

To analyze results, test logs, audit data, and feedback from test users, they were consolidated in Microsoft Excel and Power BI dashboards for visualization. Comparisons were made between baseline measurements and post implementation data to demonstrate improvements in access control enforcement, threat detection visibility, and governance readiness. The final evaluation was summarized in a results report that was presented to stakeholders alongside the Zero Trust roadmap, providing transparency and clear evidence of success aligned with national cybersecurity frameworks (NIST, 2020; CISA, 2023).

I. References

CISA. (2023). Zero Trust Maturity Model Version 2.0. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2023-04/CISA-ZTMM_V2_FINAL.pdf

CrowdStrike. (2023). Zero Trust: Adopting a Threat-Centric Approach. https://www.crowdstrike.com/resources/white-papers/zero-trust/

Google. (2020). BeyondCorp: A New Approach to Enterprise Security. https://cloud.google.com/beyondcorp

Microsoft. (2023). Microsoft 365 E5 Security licensing and pricing. https://www.microsoft.com/en-us/microsoft-365/compare-microsoft-365-enterprise-plans

Microsoft. (2023). Microsoft Sentinel pricing. https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/

Microsoft. (2023). Microsoft Zero Trust Guidance and Best Practices. https://learn.microsoft.com/en-us/security/zero-trust/

MITRE. (2023). MITRE ATT&CK Framework. https://attack.mitre.org/

NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Palo Alto Networks. (2023). The Enterprise Roadmap to Zero Trust. https://www.paloaltonetworks.com/resources/whitepapers/enterprise-roadmap-to-zero-trust