**Case Study 4:** Cyber Exposure Strategy Design and Architecture Workshop (Financial Services end customer)

**Objectives:** Design a scalable cyber exposure strategy and architecture to unify visibility, define governance, and guide phased, secure platform adoption.

**Delivery Format/Engagement Date:** Remote/February 2025

## Client Overview

Leading cybersecurity firm, publicly-traded

## End Customer Overview

The vendor's end customer, Financial Corporation is a prominent consumer financial services provider operating across multiple U.S. states. With an increasing reliance on cloud infrastructure, a distributed hybrid IT environment, and a growing regulatory burden, the customer needed a cohesive strategy to gain visibility, improve security maturity, and reduce risk across its attack surface.

The customer had already licensed multiple products, including web app scanning, cloud security, and attack surface management, but sought guidance in designing an enterprise-ready architecture, assigning operational responsibilities, and developing a roadmap for scalable deployment.

## Engagement Objectives

The goals of the engagement were to:

- Design a unified deployment strategy aligned with business priorities, operational models, and regulatory obligations.
- Establish best practices for sensor placement, RBAC (Role-Based Access Control), and tagging, ensuring scalable and secure architecture across on-premises and cloud environments.
- Create a realistic, actionable roadmap for phased adoption of different security tools, optimizing visibility and coverage.
- Empower cross-functional teams with the knowledge and ownership required to operate and extend the platform autonomously post-engagement.

## Strategic Priorities

During the planning and delivery stages, Financial Corporation articulated a clear set of outcomes they hoped to achieve:

- **Consolidated Vulnerability Management Strategy:** Integrating vulnerability insights across AWS, Azure, and on-prem assets with clear scanning roles and windows, credentialed scan policies, and CVSSv3 (Common Vulnerability Scoring System version 3) scoring.
- **Mature Role-Based Access Controls (RBAC):** Designing a multi-tiered access framework supporting InfoSec, Infrastructure, and DevOps roles while minimizing over-permissioned access.
- **Secure Identity and Active Directory Integration:** Laying the foundation for future adoption of cybersecurity tools, particularly to address risk from legacy AD infrastructure and potential lateral movement paths.
- **Cloud Visibility and Compliance Readiness:** Aligning cloud security software capabilities with Financial Corporation's CI/CD (Continuous Integration / Continuous Delivery) pipelines, SAML/IdP (Identity Provider) architecture, and public cloud governance strategy.
- **Web App Scanning Expansion:** Supporting internal application scanning via an on-prem scanner, with a plan for future coverage expansion using DAST principles.

## Approach

We were engaged by the vendor to lead this architecture workshop and roadmap design for their customer. Our team delivered a structured Vulnerability Management Design & Architecture Workshop across three phases:

### 1. Preparation & Planning

The engagement started with a stakeholder alignment call to confirm licensed entitlements, discuss technical readiness, and establish the workshop schedule. Financial Corporation designated participants from cybersecurity, infrastructure, and cloud engineering to ensure comprehensive representation.

**2. Design & Architecture Workshop (2 sessions)**

Delivered via Zoom, each 5-hour workshop explored technical capabilities, organizational needs, and operational models. The discussion was highly interactive and tailored. Key activities included:

- **Network Topology Review:** Mapping existing on-prem and hybrid workloads to determine optimal scanner placement, including where to use agents vs. scanners.
- **Scanning Strategy & Credential Management:** Aligning scan windows with maintenance schedules; defining how privileged credentials would be securely stored and rotated.
- **Cloud Security Alignment:** Reviewing AWS and Azure account structures, workload onboarding methods, and existing CI/CD workflows.
- **RBAC and Tagging Policy Design:** Building a tag hierarchy mapped to business units, environments, and asset types to simplify role-specific dashboards and filters.
- **Integration Planning:** Outlining the next steps for integrations with SAML (Security Assertion Markup Language), ticketing systems, CMDBs (Configuration Management Database), and future DSPM (Data Security Posture Management) tools.

**3. Deliverables**

Following the sessions, we delivered a detailed **High-Level Design & Architecture Document** that included:

- Logical diagrams, scan architecture, and account onboarding flows
- Scanner capacity planning and sensor topology
- Tagging strategy and access control matrix
- Roadmap for phased deployment by capability and department
- Integration considerations and guidance for SIEM/ITSM alignment

## Component-Level Design Highlights

**Vulnerability Management**

- **Assets Covered:** ~750 AWS, ~950 Azure, and ~8000 on-prem devices.
- **Scan Strategy:** Differentiated scan policies between agents and scanners; cloud connector used for dynamic assets.

- **Credentialed Scanning:** Strong emphasis on depth of insight, with support for secure credential storage and rotation using preferred vaulting tools.

**Web Application Scanning (WAS)**

- **Deployment:** On-prem WAS scanner to cover internal applications.
- **Strategy:** Emphasis on conservative configuration with a plan to scale DAST maturity over time. Integration with app inventory was discussed for future automation.

**Cloud Security**

- **Onboarding:** AWS and Azure environments added for visibility; plans to integrate with SAML, CI/CD, and notification tools.
- **DSPM Readiness:** Positioned a Cloud Security CNAPP Tool to help CNG identify data exposure risk and prioritize high-value workload protection.

**Identity Exposure**

- **Foundation Laid:** Though not currently deployed, the architecture incorporated design considerations for monitoring AD configuration and risk path analysis.

**Attack Surface Management**

- **Initial Configuration:** CNG configured its domain set and validated external asset inventory.
- **Future Plans:** Expand monitoring to include brands, subsidiaries, and marketing-registered domains.

## Key Outcomes

- **Clarity & Alignment:** Cross-functional stakeholders now share a common understanding of platform purpose, data flows, and roles.
- **Operational Readiness:** Financial Corporation is positioned to operationalize the platform with well-defined scanning cadences and governance practices.
- **Actionable Documentation:** The design artifacts are being used internally for project planning, compliance documentation, and security tool alignment.
- **Future-Ready Architecture:** Financial Corporation's roadmap supports phased rollout of all software components, including cloud, web application scanning, and identity.

## End Customer Feedback

“The workshop gave us clarity not just on how to configure the platform, but on how to think about cyber risk from a strategic, enterprise-wide perspective. We're in a much stronger position today than before.”

**— Manager of Cybersecurity, Financial Corporation**

**Address:**
1000 Brickell Av, Suite 1015
Miami, FL 33131

**Phone:**
+1 (786) 397-0480

**Maill:**
info@cyopspartners.com