Case Study 2: Identity Risk Detection and AD Hardening Initiative (IT Infrastructure end customer)

Objectives: Deploy and configure an identity exposure platform for Active Directory risk visibility, alerting, and team enablement with integration into existing security workflows.

Delivery Format/Duration: Remote/2 weeks

Client Overview (Vendor)

Leading cybersecurity firm, publicly-traded

End Customer Overview

US leading provider of enterprise-grade IT infrastructure and managed services. As identity-based threats grow in complexity and frequency, the company recognized the need to harden its Microsoft Active Directory (AD) environment—one of its most critical IT backbones.

The end customer selected the vendor's Identity Exposure Security Tool to gain continuous visibility into Active Directory risk and misconfigurations. To accelerate time-to-value and ensure internal teams were ready to operationalize the platform, the customer engaged our team to deliver a deployment engagement focused on visibility, configuration, alerting, and training.

Engagement Objectives

- **Install and configure Identity Exposure Security Tool** components including Secure Relay, Directory Listener, Security Engine, and Storage Manager
- **Integrate Identity Exposure Security Tool with the customer's AD domain** and validate visibility across all required protocols such as LDAP (Lightweight Directory Access Protocol), SMB (Server Message Block), Kerberos, RPC (Remote Procedure Call)
- **Create initial users, security profiles, and alerting rules** using LDAP authentication, SMTP (Simple Mail Transfer Protocol) notifications, and SYSLOG (System Logging Protocol) forwarding
- **Customize dashboards, policies, and threat detection settings** to reflect the customer's unique AD layout and administrative structure

- **Enable the internal team through hands-on workshops**, real-time usage, and a strategic roadmap for next-phase success

Strategic Priorities

- **Establish Non-Intrusive Visibility Across the AD Environment:** The customer needed a passive, low-latency method to monitor AD misconfigurations and exposure pathways without relying on intrusive scanning or excessive network overhead.
- **Operationalize Identity-Based Threat Detection:** The security team was focused on surfacing both Indicators of Exposure such as outdated password policies and excessive privileges, and Indicators of Attack including unauthorized GPO changes and lateral movement signals.
- **Integrate into Existing Toolchains:** The customer needed to feed alert information into the organization's existing SYSLOG/SIEM pipeline and deliver secure, actionable notifications via Microsoft 365's SMTP infrastructure.
- **Enable Self-Sufficiency Across Teams:** From the beginning, the customer emphasized the need to build long-term internal capability, with administrators expected to configure, tune, and manage the platform after the engagement.

Approach

We delivered the deployment remotely over two weeks, with collaborative working sessions and phased delivery aligned to best practices and the customer's operational environment. We were engaged by the vendor to lead this deployment on their behalf.

1. Infrastructure Configuration and Installation

- Deployed the communication bridge on a hardened Windows Server 2019 virtual machine with 2 vCPUs, 8 GB RAM, and 30 GB storage
- Installed the Directory Listener, Security Engine Node, and Storage Manager, verifying full health and encrypted connectivity across all nodes
- Integrated the platform with:
    - LDAP-based authentication for role-based access
    - SMTP notifications using smtp.office365.com with StartTLS
    - SYSLOG alert forwarding for integration with the customer's external SIEM

2. AD Domain Integration and Protocol Verification

- Connected the security tool to the AD forest and validated ingestion across key protocols (Kerberos, SMB, RPC)
- Ensured directory object visibility including trust relationships, protected groups, GPOs (Group Policy Object), and replication metadata
- Tested permissions to Recycle Bin and Password Settings Container for full exposure analysis

3. User Setup and Role-Based Access Control

- Created TIE user accounts and assigned roles:
  - Global Administrators
  - Scoped access groups created for future teams
- Implemented Full Access Groups to segment visibility by business function or asset scope
- Assigned permissions for dashboard viewing, Trail Flow usage, and profile editing

4. Dashboard and Trail Flow Enablement

- Delivered interactive instruction on the security tool, with exercises on:
  - Tracking GPO changes
  - Visualizing group membership expansion
  - Detecting anomalous logins or time-of-day deviations
  - Reviewing attack signatures related to lateral movement and data staging
- Deployed three default dashboards and guided the customer in editing views for AD exposure maps, blast radius detection, and policy deviation

5. Indicators of Exposure and Indicators of Attack Customization and Alerting

- Reviewed and contextualized key IoEs (Indicators of Exposure) surfaced by the platform, such as:
  - Insecure Netlogon paths
  - High-privilege users with unconstrained delegation
  - Deprecated cryptographic standards in password policies
  -

- Enabled active monitoring for IoAs (Indicators of Attack), including:
  - Executable drop events in SYSVOL
  - Suspicious registry changes linked to persistence
- Configured and validated SMTP and SYSLOG alerts, with customized thresholds for critical exposures and deviations

6. Strategic Roadmap and Recommendations

- Delivered a customer-specific improvement plan, including:
  - Regular Flow-based investigations into high-risk changes
  - Continuous review of protected group memberships (e.g., Domain Admins, Schema Admins)
  - Ongoing refinement of dashboards and widgets using export/import templates
  - Participation in official training for continued enablement
  - Planning for a post-deployment Health Check in 6–12 months

Results & Impact

- **Full Identity Exposure Visibility Achieved in Days:** The customer quickly surfaced critical AD exposures, from misconfigured trust relationships to excessive privilege assignments.
- **Operational Threat Monitoring Enabled:** With dashboards, Trail Flow, and alerting in place, the team began daily monitoring routines supported by real-time alerts and weekly dashboards.
- **Security Team Empowered for Ownership:** Admins participated directly in platform setup, tuning, and use-case development, reducing reliance on external support.
- **Platform Integrated into Broader Ecosystem:** Alert forwarding and SMTP notification tied TIE into existing workflows—without requiring disruptive changes to other tools.
- **Strategic Momentum Secured:** the end customer internal teams now have both the tools and the roadmap to evolve their identity security program from reactive analysis to proactive prevention.

End Customer Feedback

“The Identity Exposure Quick Start gave us immediate visibility into risks we couldn’t previously detect. Now we not only see our exposure, but we know exactly how to address it—and we’re doing it with a trained team and real-time alerting.”

— **Security Program Manager**, Infrastructure Solutions customer