ACTIVE DIRECTORY HARDENING

OVERVIEW

Identity is the new security perimeter. Whether your assets are hosted on-premises or in the cloud, the security "perimeter" that separates users and data from outside threats can no longer be drawn using network lines. The security "perimeter" to defend between your assets/users and threats is drawn by Identity components of authentication and authorization that span across all your devices, services, hosts, and networks.

Modern cybersecurity threats routinely compromise privileged identities which grant control to corporate and government computing environments. When these malicious attacks are successful, they can gain full access to most or all of an organization's electronic documents, presentations, applications, databases, and other highly sensitive information or assets. Therefore, it is important for an organization to understand the potential ways unauthorized users could gain Administrator level access.

IntraSystems' Active Directory Hardening (ADH) engagement is designed to discover and analyze privilege account exposure and provide transition assistance for deviations from Microsoft's privileged administration recommendations. The ADH does this by reducing the number of highly privileged Active Directory administrative accounts and moving them into a recommended Active Directory administration model.

By conducting an Active Directory Hardening (ADH) engagement, you'll be able to reduce credential exposure and upgrade to a modern administrative architecture:

- 75% of all network intrusions result from comprised user credentials
- $3.5M of cost/business impact per breach
- 200+ median number of days that attackers reside within a victim's network before detection

PROCESS

IntraSystems' ADH engagement includes a four-day engagement with an IntraSystems' Active Directory Architect working with the customer's Security and Active Directory staff. The deliverables will consist of training, knowledge transfer and implementation of the recommended mitigations in a customer test environment:

DAY 1	**TRAINING** ▪ Discuss current trends observed in today's threat ▪ Discuss different mitigations to reduce the risk of Credential Theft Attacks ▪ Discuss a number of GPO settings to help manage highly privileged local groups and restrict local groups ▪ Review current threat landscape and PAW design concepts and deployment options ▪ Discuss utilizing the Microsoft LAPS product for randomizing local administrator passwords
DAY 2	▪ Demonstrate Tier model environment to customer
DAY 3	▪ Implement Microsoft PAW in customer's test lab environment
DAY 4	▪ Implement Microsoft LAPS in customer's test environment to create unique passwords for the local administrator accounts on all machines

IntraSystems follows Microsoft's Reference Architecture for Active Directory Administration. The purpose of this tier model is to protect identity systems using a set of buffer zones between full control of the environment (Tier 0) and the high-risk workstation assets that attackers frequently compromise.

TIER 0	**Domain & Enterprise Admins** ▪ Domain Controllers ▪ Systems which operate or manage Domain Controllers ▪ Accounts which access or administrate any of the above
TIER 1	**Server Admins** ▪ Member servers and administrators ▪ Enterprise application administrators ▪ Cloud service administrators
TIER 2	**Workstation & Device Admins** ▪ Helpdesk support ▪ Device support ▪ User support

By completing this engagement, you'll be able to:

- Understand the tools that are used carry out Credential Theft Attacks
- Understand the breadth of related credential theft risks
- Understand the specific risks of shared passwords and available mitigations
- Deploy mitigation easily in a lab with a custom PowerShell module
- Create an OU structure that is aligned to the best practices in the Microsoft DIAD model
- Enforce local account restrictions for remote access

ABOUT US

Founded in 1996, IntraSystems is a highly respected IT consulting/advisory firm, managed services provider, and systems integrator with SOC 2 and ISO 27001 certifications. Specializing in IT infrastructure deployment, cybersecurity services and assessments, virtualization, security, and cloud solutions, IntraSystems excels at addressing today's complex technology challenges. From navigating the rapidly evolving security landscape to cloud migration and meeting compliance standards like GDPR and HIPAA, IntraSystems delivers proven expertise and tailored solutions everytime.

IntraSystems ensures customer satisfaction through technical expertise, strong partnerships, and the professional integrity of every team member. With specialized knowledge and experience that is hard to replicate, we build trusted relationships and deliver the industry's highest level of personalized service. By combining in-house expertise with top-tier business partnerships, IntraSystems empowers your organization to focus on its core business priorities.

We assess your business priorities and environment to identify the ideal combination of technical expertise and technology tailored to your unique needs. Recommending, customizing, and implementing IT solutions are at the core of our strengths. Over the years, our commitment to service and our reputation for technological and business integrity have earned us an extensive list of satisfied clients. We take our responsibility very seriously. It's an approach that works well in everyday situations — and it's precisely what drives our success.

LEARN MORE

Schedule your Active Directory Hardening engagement now! Visit our website at www.intrasystems.com or contact our sales team at sales@intrasystems.com or 781.986.1700.

35 BRAINTREE HILL OFFICE PARK, SUITE 403 | BRAINTREE, MA 02184 | 781.986.1700 (T) | 781.986.1001 (F)
SALES@INTRASYSTEMS.COM WWW.INTRASYSTEMS.COM