IOT Identity & Access Management Team - 2021

Who We Are:

A 6-member team that supports and maintains identity and access service technology infrastructure for all supported State agencies as well as their business partners and constituents.

Our Mission:

The IOT Enterprise Identity Services team works to provide enterprise grade authentication and access control needs to all State of Indiana supported Agencies and where applicable business partners and customers. Nearly every service or modern business process integrates with our Active Directory based infrastructure offerings. Therefore, we strive to increase productivity across platforms through modern SSO opportunities yet keep data and identities secure and highly available.

Located: IGCN – 5th Floor.

Department: 493014

Manager: Patrick Evans

What We Do:

Manage Active Directory (AD) domain services for the organization, which is the backbone for authentication and name resolution (DNS). The AD team is responsible for design, implementation, security hardening, disaster planning, recovery, management and troubleshooting of Active Directory infrastructure issues. In addition to Active Directory, we also maintain Azure Active Directory for use with Azure AD integrated applications including Office 365 as well as ADFS, MFA, Azure AD B2B and B2C services.

Our Products:

Microsoft Active Directory, Microsoft Active Directory Federation Services, Microsoft Azure Active Directory, Microsoft Azure Active Directory B2B, Microsoft Azure Active Directory B2C, Microsoft AD Connect, Microsoft MFA Server, Microsoft Identity Management Server

Our Tools: ASM Ticket Management and SLA Measurement

Our Metrics: Resolve customer issues within 2 IOT business days 90%+ G; 87%+ Y; <87% R
Mon-Fri 6am-6pm excluding state holidays

Our Customers:

39,000 state employees and contractors, 5000+ Service and resource accounts, 6000 Guest business partner accounts and 500000 constituent B2C accounts.

Our Budget: Please see Seat

Major Accomplishments:

- Designed and implemented a complete Enhanced Secure Administration Environment (ESAE) to allow secure Active Directory Tier 0 administration (Sometimes referred to as "Red Forest").
- Working with IOT Office of the CTO and MPH, Designed and implemented external "Enhanced Research Environment" utilizing Azure AD Domain Services and Windows Virtual Desktop.
- With knowledge gained from MPH ERE work, we worked quickly with the IOT Office of the CTO, Desktop and Automation team to quickly provision Microsoft WVD services for remote work aid in the State's COVID-19 workforce response.
- Designed an enterprise single sign-on (SSO) solution for Azure AD and Office 365, paving the way for further application integration.

Current Projects:

- Active Directory Domain Hardening, this is a project that has been in work and continues. Based on Microsoft best practices, we are fixing security issues within our large complex active directory forest. The work is slow and difficult due to the impacts across our users, services, applications and infrastructure and the required work with all the stakeholders regarding the changes involved.
- Azure AD security hardening. This will make sure we are integrating Azure AD in line with security best practices. Includes token lifetime evaluation, conditional access, least privilege access and proper role-based access provisioning.
- Certificate Authority infrastructure upgrades. This is a large project in which a new Certificate Authority will be designed and created from scratch using modern security best practices and principles.
- Design and document Active Directory Disaster Recovery plan specific to the State of Indiana for all production AD environments based on new best practices provided by Microsoft.