Lack of control over privileged access to systems and data presents a significant risk to almost every organization. What is required to protect privileged accounts? Are you in control? Do you have an effective Privileged Access Management (PAM) program? In this session, we will discuss:

1. Assessing current state of your PAM program and defining a target state
2. Developing a roadmap to implement your desired target state
3. Selecting the right PAM solution to help you gain better control over privileged access
PRIMER: WHAT IS PRIVILEGED ACCESS MANAGEMENT?

Privileged Access Management (PAM) is maintaining control and visibility over creation and use of accounts with elevated access to critical systems and data.
TYPES OF PRIVILEGED ACCOUNTS

- Domain and Local Admin Accounts
- Privileged User Accounts
- Emergency Accounts
- Application Accounts
- Service Accounts
WHAT ARE THE KEY RISKS OF PRIVILEGED ACCOUNTS?

**Static Credentials**
Passwords are rarely changed and credentials are nearly impossible to disable due to a high potential for disruption.

**Anonymous Logins**
Due to its shared nature, the privileged account carries no personal accountability.

**“Least Privilege” Violation**
Many privileged accounts provide full access to systems and data.

**Pervasive Misuse**
In most organizations, there are hundreds, if not thousands, of privileged accounts.

**Shared Accounts**
Privileged accounts are often generic accounts that are shared between multiple individuals.
PRIVILEGED ACCOUNTS ACROSS THE STACK

- Data Security
- Application Security
- End-Point Security
- Network Security
- Cloud Security
SECTION 1: CURRENT STATE ASSESSMENT

01 Assessing current state of your PAM program and defining a target state

02 Developing a roadmap to implement your desired target state

03 Selecting the right PAM solution to help you gain better control over privileged access
ASSESS CURRENT STATE MATURITY

Inventory & Governance

- Privileged account inventory and ownership
- Policies and procedures for protection of privileged accounts
ASSESS CURRENT STATE MATURITY

Control & Monitoring
- Safeguards for protection of privileged accounts
- Practices for logging and monitoring the usage of privileged accounts

Inventory & Governance
- Privileged account inventory and ownership
- Policies and procedures for protection of privileged accounts
ASSESS CURRENT STATE MATURITY

PAM Lifecycle & Tools
- PAM lifecycle processes (access request, approval, provisioning, and recertification)
- PAM tools and privileged account authentication

Control & Monitoring
- Safeguards for protection of privileged accounts
- Practices for logging and monitoring the usage of privileged accounts

Inventory & Governance
- Privileged account inventory and ownership
- Policies and procedures for protection of privileged accounts
ASSESS CURRENT STATE MATURITY

PAM Integration

- Risk Assessments
- Identity & Access Mgmt.
- Change Management
- Incident Response

PAM Lifecycle & Tools

- PAM lifecycle processes (access request, approval, provisioning, and recertification)
- PAM tools and privileged account authentication

Control & Monitoring

- Safeguards for protection of privileged accounts
- Practices for logging and monitoring the usage of privileged accounts

Inventory & Governance

- Privileged account inventory and ownership
- Policies and procedures for protection of privileged accounts
DEFINE DESIRED TARGET STATE MATURITY

Current State Maturity → Compliance Requirements → Desired State Maturity
DEFINE DESIRED TARGET STATE MATURITY

Baseline Maturity

- Inventory and reduce the number of privileged accounts in your organization
- Prohibit standard user accounts from having privileged access.
- Create a process for on- and off-boarding employees that have privileged account access.
- Eliminate the practice of accounts that have non-expiring passwords.
- Store passwords securely.
- Ensure, to the best of your ability, all actions using shared administrative accounts can be attributed to a specific individual.
DEFINE DESIRED TARGET STATE MATURITY

Medium Effective Maturity

- Automatically change privileged account passwords on a 30 to 60 day cycle.
- Utilize one-time passwords, which are passwords that are valid for only one login session or transaction.
- Implement session recording for key assets, servers, and third party access.
- Eliminate the option of interactive (human) login for service accounts.
- Implement a process to change hard-coded or embedded passwords for scripts and service accounts.
- Implement focused auditing on the use of administrative privileged functions and monitor for irregular behavior.
DEFINE DESIRED TARGET STATE MATURITY

Highly Effective Maturity

- Use automated tools to disable inactive privileged accounts.
- Use multifactor authentication for all administrative access, including domain administrative access.
- Implement automated password verification and reconciliation to ensure that the password of record are current on all systems.
- Regularly change and verify hardcoded passwords embedded in applications.
- Deploy a solution that provides the ability to directly connect to a target system without displaying the password to the user.
- Implement a gateway to eliminate privileged users directly accessing sensitive assets in the IT infrastructure.
- Implement a request workflow for credential access approval including dual-controls and integration with helpdesk ticketing systems.
- Implement session recording for all privileged access.
SECTION 2: DEVELOP THE ROADMAP

01 Assessing current state of your PAM program and defining a target state

02 Developing a roadmap to implement your desired target state

03 Selecting the right PAM solution to help you gain better control over privileged access
THE ROAD TO AN EFFECTIVE PAM PROGRAM

Program Maturity
- Reduce reliance on manual processes by automating PAM capabilities.
- Implement analytics to better understand and monitor the usage of privileged accounts.

Strategic Planning & Governance
- Establish a formal governance structure and assign ownership across the organization.
- Define a target operating model with clearly defined policies, procedures, roles and responsibilities.
- Get management buy-in and funding.

Program Operationalization
- Establish a continuous process to discover, evaluate the effectiveness of controls, remediate gaps, and monitor the use of privileged accounts.
- Develop a scalable solution architecture that addresses your needs in the current and future state.

PAM Integration
- Integrate privileged account management practices and technologies across the enterprise.
SECTION 3: PAM SOLUTIONS

01. Assessing current state of your PAM program and defining a target state

02. Developing a roadmap to implement your desired target state

03. Selecting the right PAM solution to help you gain better control over privileged access
PAM solutions help organizations gain better control over privileged access. PAM solutions are composed of technical components that work together to solve different aspects of the privileged access management challenge. PAM solutions can be divided into four functional categories:

- **Privilege Session Management (PSM)**
- **Superuser Privilege Management (SUPM)**
- **Shared Account Password Management (SAPM)**
- **Application-to-application password management (AAPM)**
SHARED ACCOUNT PASSWORD MANAGEMENT (SAPM)

**Key Controls:**
- Privileged password management
- Password vault
- Administrator password check-out
- Session initiation
- Emergency access
- Audit and reporting

**Reduce the Risk Through:**
- Elimination of static, shared and well-known passwords
- Linking privileged account access to specific individual users
- Policy-based controls that manage access to sensitive information
- Integration with strong authentication technologies
- Detailed audit trail
PRIVILEGED SESSION MANAGEMENT (PSM)

Key Controls:

- Session management
- Session recording
- Real-time monitoring
- Analysis, reporting, alerting and notifications

Reduce the Risk Through:

- Creating centralized control for accessing all privileged accounts
- Detailed session recording suitable for forensic analysis and investigations
- Real-time alerts for known high-risk events
SUPERUSER PRIVILEGE MANAGEMENT (SUPM)

Key Controls:
- Privilege and user delegation
- Containment
- Role-based access control
- Centralized policy management
- Command filtering
- Auditing and reporting

Reduce the Risk Through:
- Enforcement of the principle of least privilege
- Centralized policy-based management of roles
- Context-sensitive filtering of commands for fine-grained access control
APPLICATION-TO-APPLICATION PASSWORD MGMT (AAPM)

Key Controls:
• Application-to-application password management
• Application-to-application account discovery
• Password vault
• Programmatic password check-out
• Audit and reporting

Reduce the Risk Through:
• Elimination of hard-coded and embedded clear-text passwords
• Policy-based controls to manage access
• Detailed audit trail
WRAP UP

01. Use a risk-based approach to plan your PAM initiatives. This will enable you to focus on protecting critical assets and implementing an optimal set of controls.

02. Allocate time and resources for the discovery phase to understand your risks and accommodate for IT’s operational needs. This will position you for a successful PAM implementation.

03. Integrate PAM solutions with core identity governance and administration components and security information and event management (SEIM) tools to improve preventative and detective controls.
Q&A
Face the Future with Confidence
**Speaker Bio**

**Stevens, Katie:** Katie has spent her 15+ years in technology solving complex business problems including Business Continuity Management and Identity & Access Management. Most recently, she’s been leading readiness reviews and creating strategies to address the EU’s General Data Protection Regulation (GDPR) at global firms across a diverse set of industries. She’s currently an Associate Director for Protiviti’s Security Practice in Chicago.

[Email: katie.stevens@protiviti.com](mailto:katie.stevens@protiviti.com)