GOVERNMENT SERIES

Service Account Management

Operational risk – defined by three items: Mission Impact, Threat, and Vulnerability. The Thycotic solution helps pass Command Cyber Operational Readiness Inspections (CCORI) audits.

Background

Command Cyber Operational Readiness Inspections (CCORI) audits - Service accounts are a high-risk area and many DoD groups fail CCORI audits. Service account management is a task that is all too often overlooked as the accounts can be difficult for organizations to manage. Especially across multiple accounts for different services and applications, which need to be in sync.

Thycotic has a solution:

Customer Success Story (US Navy)

Fleet Cyber Command / 10th Fleet red team and blue team performed a Command Cyber Operational Readiness Inspection (CCORI) audit at Navy. They passed the audit and kept network integrity for domain and service accounts after considerable time was spent by red team trying to identify vulnerabilities to access the network. Thycotic Secret Server is in use on these networks along with procedures initiated by the main POC. They passed with flying colors by implementing a timed "break glass" process of one-time passwords using Thycotic Secret Server that was able to secure key accounts and ensure protection.

Secure and govern service accounts that run critical IT systems.

- The first step in managing service and system accounts is finding accounts you don't know exist.
- IT may not be able to inventory all accounts due to manual processes or error.
- By implementing the Thycotic solution, automatic discovery and management of service accounts become simple.

Capabilities

Establish a Secure Vault – Store privileged credentials in an encrypted, centralized vault.

Discover Privileges – Identify all service, application, administrator, and root accounts to curb sprawl and gain full view of your privileged access.

Manage Secrets – Provision and deprovision, ensure password complexity, and rotate credentials.

Delegate Access – Set up RBAC, workflow for access requests, and approvals for third parties.

Control Sessions – Implement session launching, proxies, monitoring, and recording

Overview

Secret Server can manage your service accounts to automatically change the passwords on a regular schedule. Using Discovery for service accounts allows Sys Admins to scan the network to:

- Find all the service accounts on your network and the dependent services, tasks, and app pools
- Determine where each service account is being used (including new usages since last scan)
- Import all service accounts into the Secret Server repository for management and auditing

Discovery for service accounts reduces manual errors and omissions in managing these accounts, sets up an audit trail for all service accounts, tracks usage, and simplifies the management process.

Risk Factors

- Service accounts are used to run various services.
- Managing passwords on these service accounts (or application accounts) is difficult
- May be leaving backdoor accounts in place allowing users to bypass controls and auditing.
- External threats may create user accounts for later access that can go undetected for months.

Contacts

Ross Johnson,
Director of Public Sector
ross.johnson@thycotic.com
(281) 804.7021

Jay Pyburn,
AE for DoD and IC
jay.pyburn@thycotic.com

(954) 579.7087

Compliance & Accreditation

- Common Criteria - US Schema
- Navy DADMS ID: 10668
- FIPS 140-2 crypto module available
- FISMA, NIST SP 800-53
- DFARS, and ISO 27001
- Federal Identity, Credential and Access Management (FICAM), and NIST's Cybersecurity White Paper targets
- Meet DISA STIGs• AES 256 encryption
- Two-factor authentication
- CAC, PIV compliance
- SIEM integration