IBM Security

Zajištění bezpečnosti privilegovaných účtů

OBJEVTE, SPRAVUJTE, CHRAŇTE A ZAZNAMENEJTE PRIVILEGOVANÉ PŘÍSTUPY VE VAŠÍ ORGANIZACI

David Hálek
Client Technical Professional – Central Region

david.halek@ibm.com

Červen 2018

IBM

Kybernetické hrozby

- 80% průniků zahrnuje **slabé nebo odcizené přihlašovací údaje**
- 54% organizací využívají **papír nebo Excel** pro řízení privilegovaných účtů
- **Neznámé a neřízené** privilegované účty
- Privilegované účty jsou známi **všem** administrátorům
- Hesla a SSH klíče jsou **statické**
- Zbytečně **vysoká oprávnění** pro privilegované přístupy

První analogie – hesla

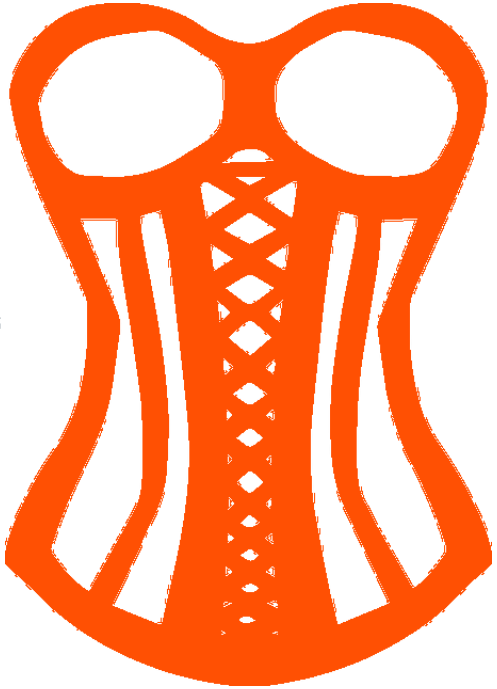
„Hesla jsou jako spodní prádlo“

1) Pravidelně je měníme za **nová**
2) Nenecháváme je **volně ležet** na stole
3) **Nepůjčujeme** je nikomu jinému!

Druhá analogie – privilegované identity

„Privilegované identity jsou jako svůdné prádlo“

1) Pouze “**někteří**“ by je měli vidět
2) Mělo by se používat pouze pro “**speciální příležitosti**“
3) Vždy je pečlivě **vrátíme** do šuplíku
4) Nahráváme pouze po udělení **souhlasu!**



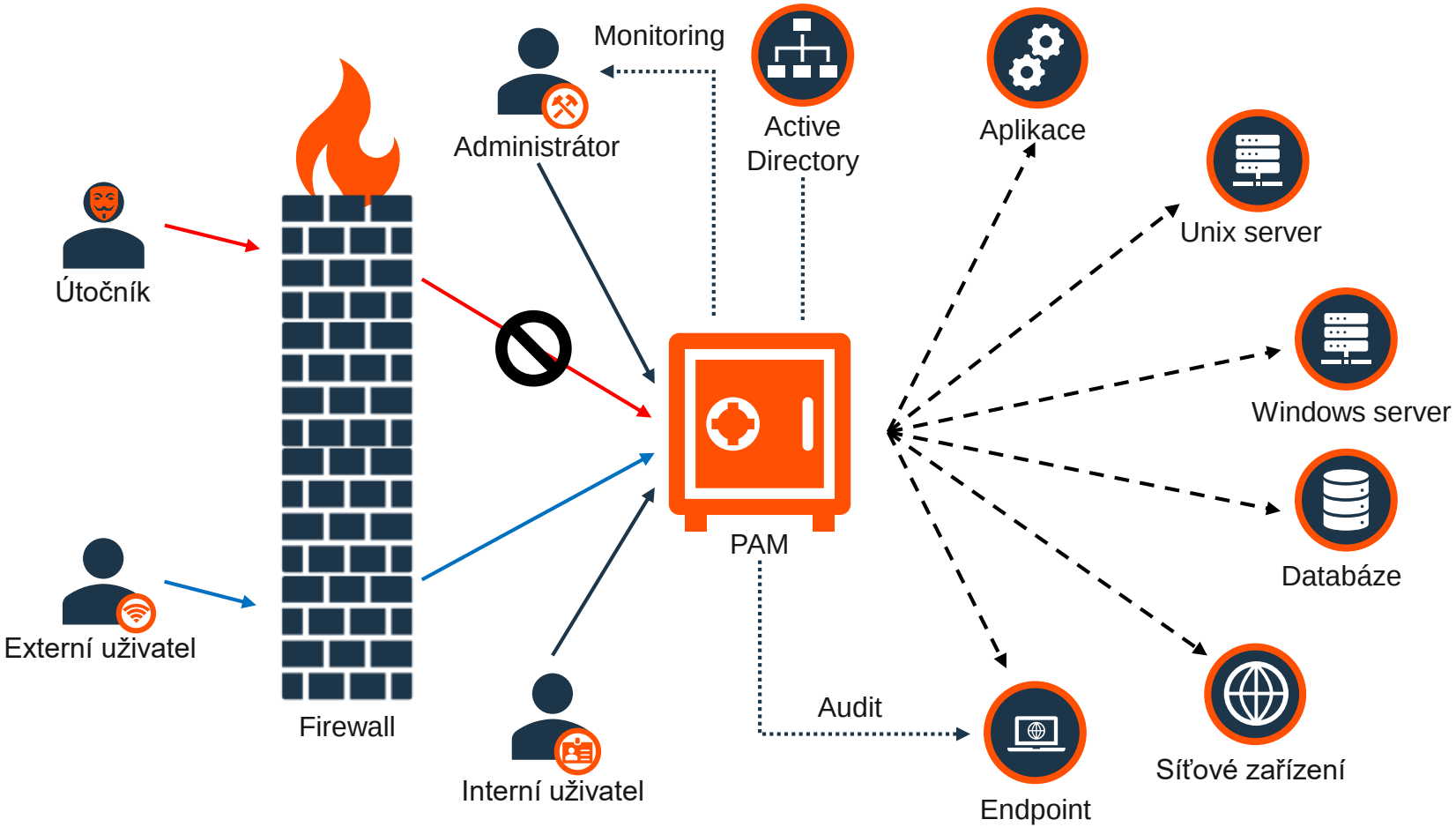
Co je to PAM?

PAM je doménou Identity & Access Mgmt. zaměřené na zvláštní požadavky na správu výkonných účtů v IT infrastruktuře podniku.

Na základní úrovni je PAM sejfem, který slouží k bezpečnému ukládání a sdílení přístupu k privilegovaným účtům.

- **Privileged Account Mgmt.**
- Privileged Access Mgmt.
- Privileged User Mgmt.
- Privileged Identity Mgmt.
- Privileged Password Mgmt.
- Privileged Account Security

S PAM řešením



IBM Secret Server – PAM řešení

JEDNODUCHÉ POUŽÍVÁNÍ | KOMPLETNÍ END-TO-END PAM ŘEŠENÍ

Správa privilegovaných účtů

Secret Server

Oprávnění aplikací

Privilege Manager

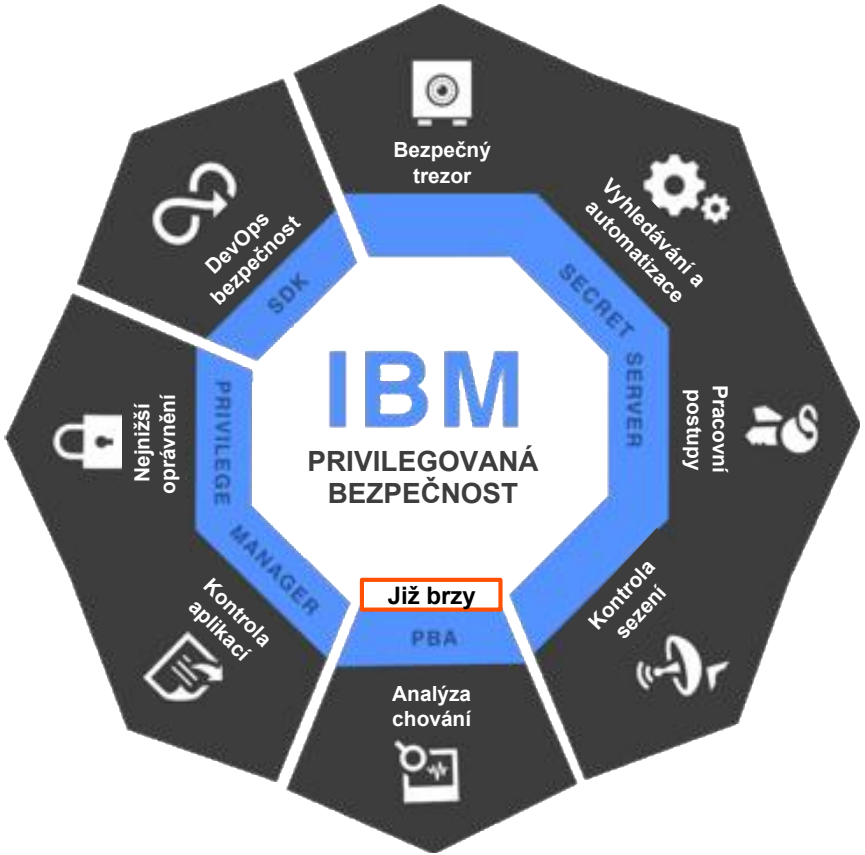
Detekce interních hrozeb

Privileged Behavior Analytics

Již brzy

Software Development Security

SDK (DevOps)



IBM Wins


وتحيا بها الحياة
add life to life


Arkansas
BlueCross BlueShield
An Independent Licensee of the Blue Cross and Blue Shield Association


OGE
OGE Energy Corp.


FREMONT
BANK


Bupa
بوبا


EDISON
EDF GROUP


KGHM
POLSKA MIEDŹ


//ABANCA


BANCO
FIBRA


espublico.


umb
you first
universal
merchant
bank


THE GREAT SEAL OF THE STATE OF OHIO


DASSAULT
AVIATION

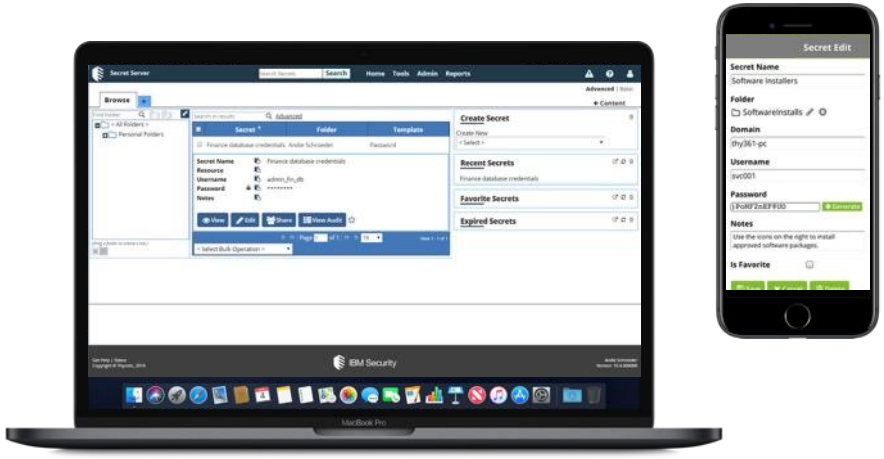

CC&G
London Stock Exchange Group


The City of Prague

Co je IBM Secret Server?

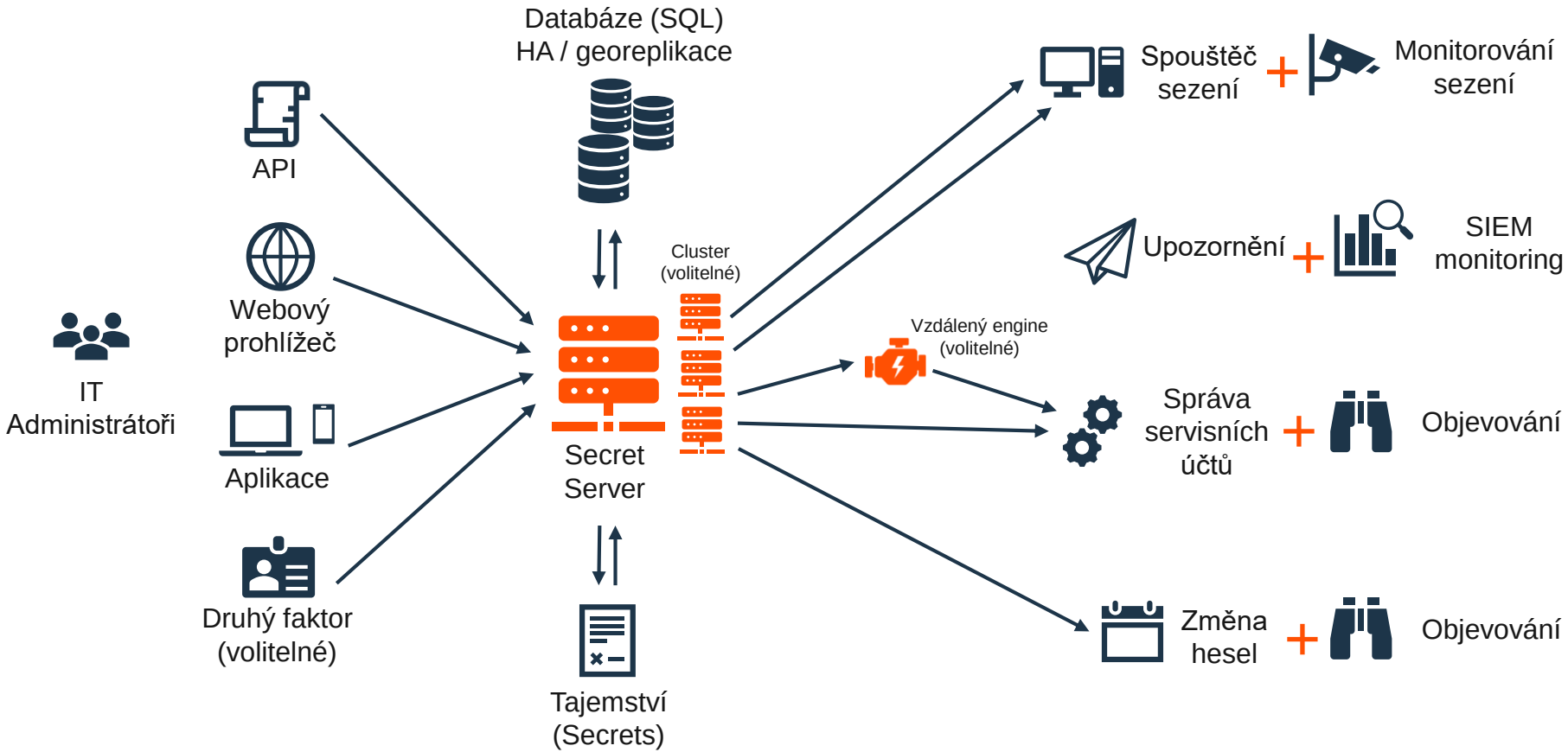
Na té **nejzákladnější úrovni** je Secret Server trezor pro bezpečné uložení a sdílení přístupu k přihlašovacím údajům privilegovaných účtů.

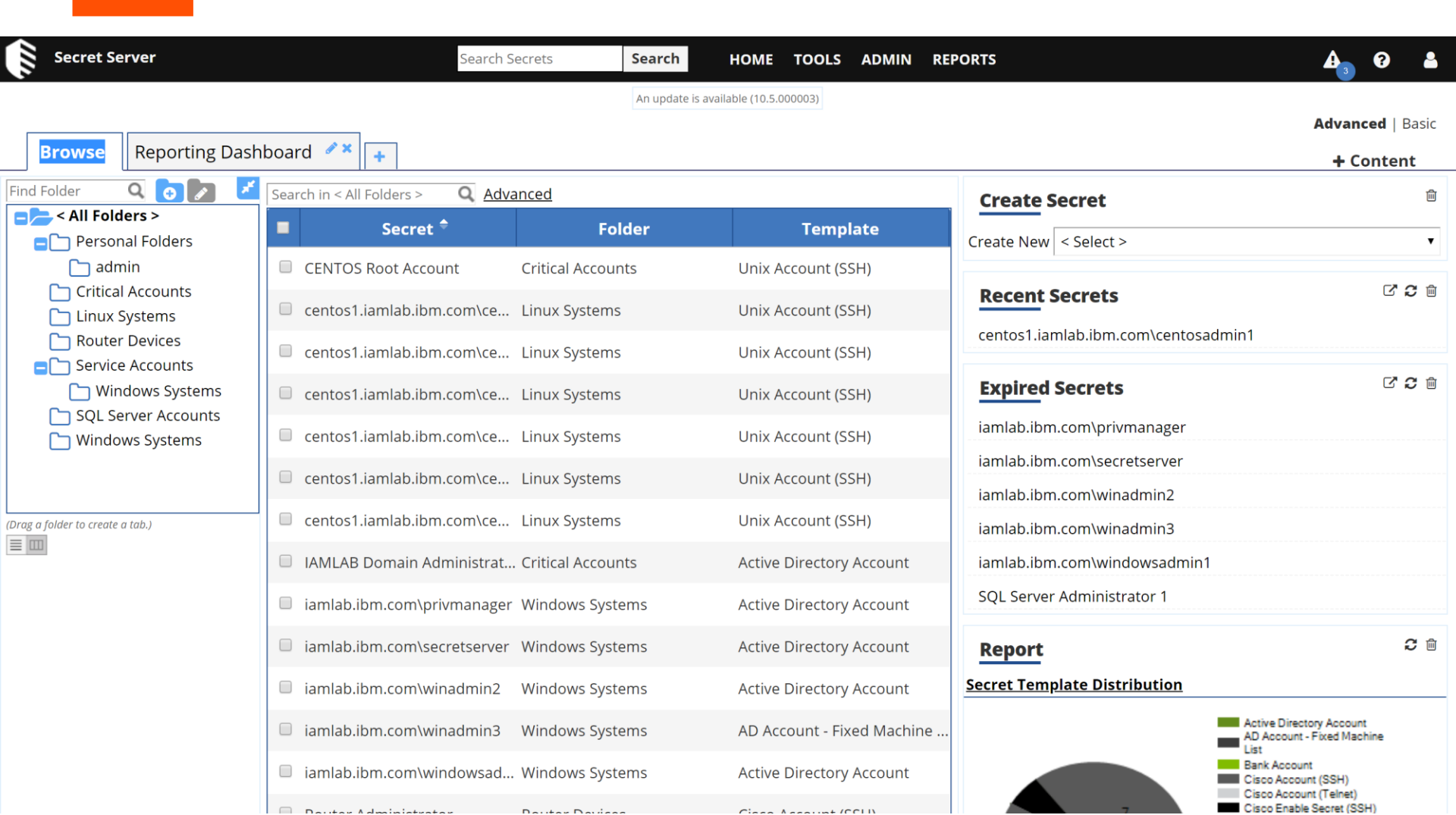
Secret Server je webová aplikace, přístupná prostřednictvím:



- libovolného webového prohlížeče
- mobilní aplikace
- API

IBM Secret Server - Architektura




Secret Server
Search Secrets
Search
HOME
TOOLS
ADMIN
REPORTS
An update is available (10.5.000003)
Advanced | Basic
Browse
Reporting Dashboard
+ Content
Find Folder
< All Folders >
Personal Folders
admin
Critical Accounts
Linux Systems
Router Devices
Service Accounts
Windows Systems
SQL Server Accounts
Windows Systems
(Drag a folder to create a tab.)
Search in < All Folders >
Advanced
Secret
Folder
Template
CENTOS Root Account
Critical Accounts
Unix Account (SSH)
centos1.iamlab.ibm.com\ce...
Linux Systems
Unix Account (SSH)
IAMLAB Domain Administrat...
Critical Accounts
Active Directory Account
iamlab.ibm.com\privmanager
Windows Systems
iamlab.ibm.com\secretserver
iamlab.ibm.com\winadmin2
iamlab.ibm.com\winadmin3
AD Account - Fixed Machine ...
iamlab.ibm.com\windowsad...
Create Secret
Create New
< Select >
Recent Secrets
centos1.iamlab.ibm.com\centosadmin1
Expired Secrets
iamlab.ibm.com\privmanager
iamlab.ibm.com\secretserver
iamlab.ibm.com\winadmin2
iamlab.ibm.com\winadmin3
iamlab.ibm.com\windowsadmin1
SQL Server Administrator 1
Report
Secret Template Distribution
Active Directory Account
AD Account - Fixed Machine List
Bank Account
Cisco Account (SSH)
Cisco Account (Telnet)
Cisco Enable Secret (SSH)

Secret Server | Search Secrets | Search | HOME | TOOLS | ADMIN | REPORTS

An update is available (10.5.000003)

Watch Session Recording

Session Summary

Session Secret: < None >
Machine: winclient1

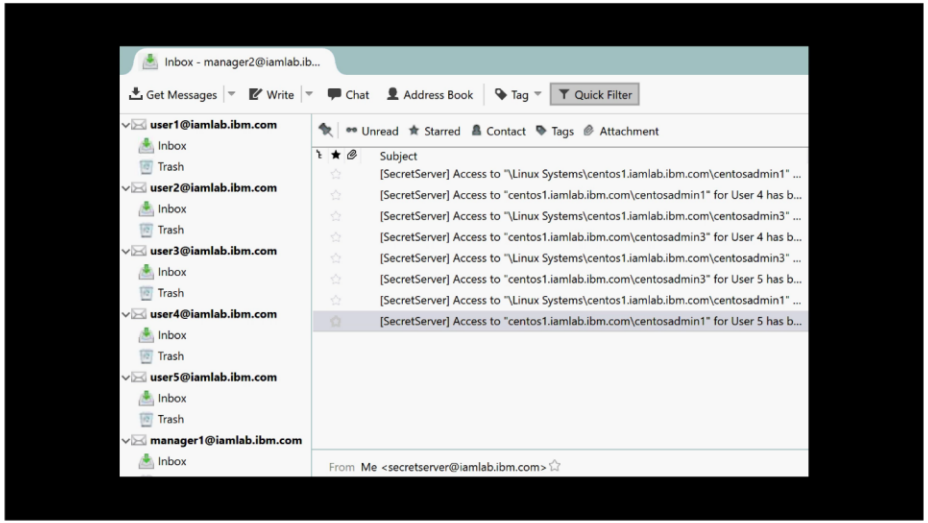
Session User: iamlab\user1
Launcher Used: < None >

Session Start: 12/20/2018 11:23 AM
Session End: 12/20/2018 11:35 AM

Search Session Activity

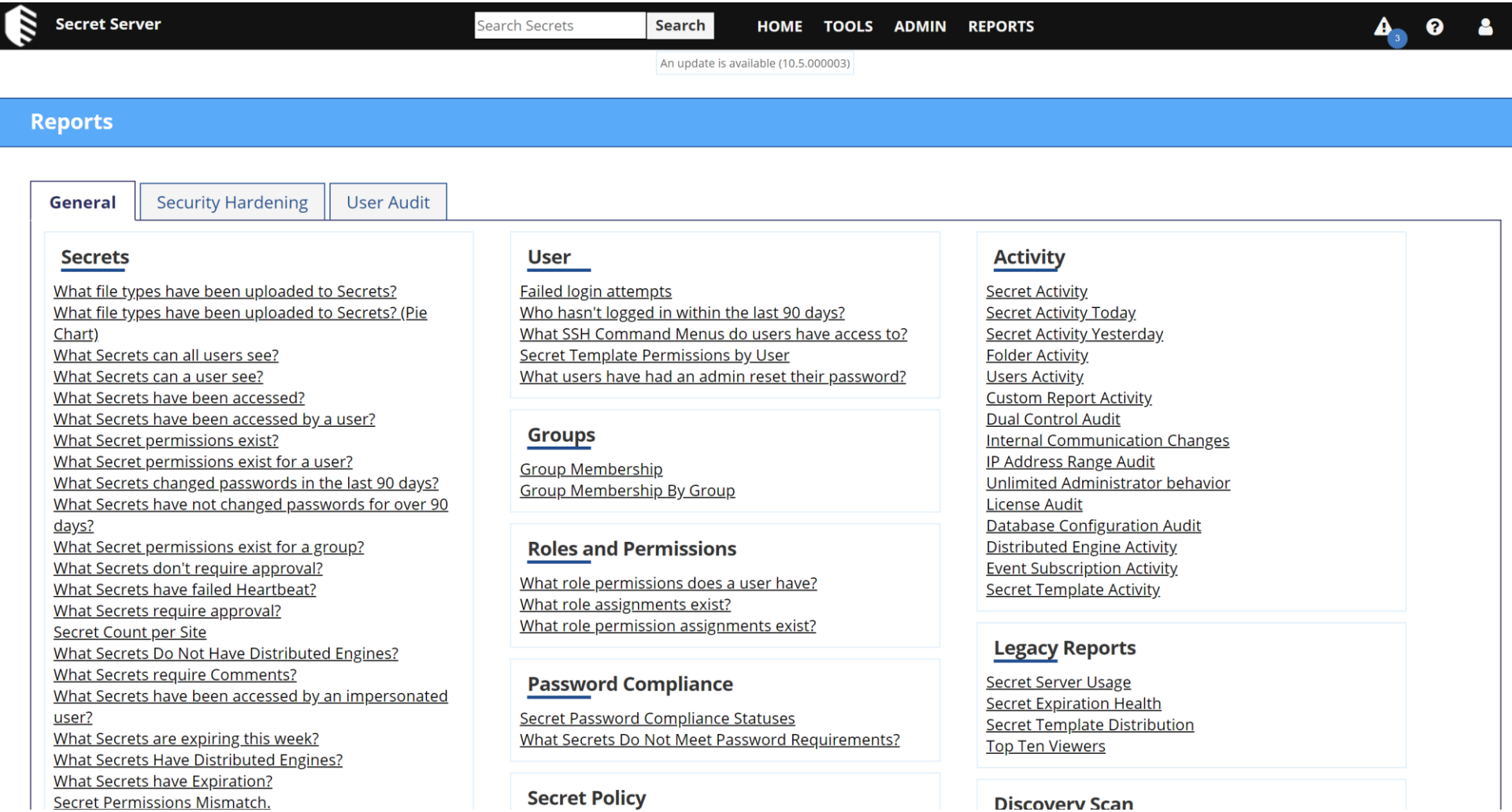
Activity Type: All | Keyword:

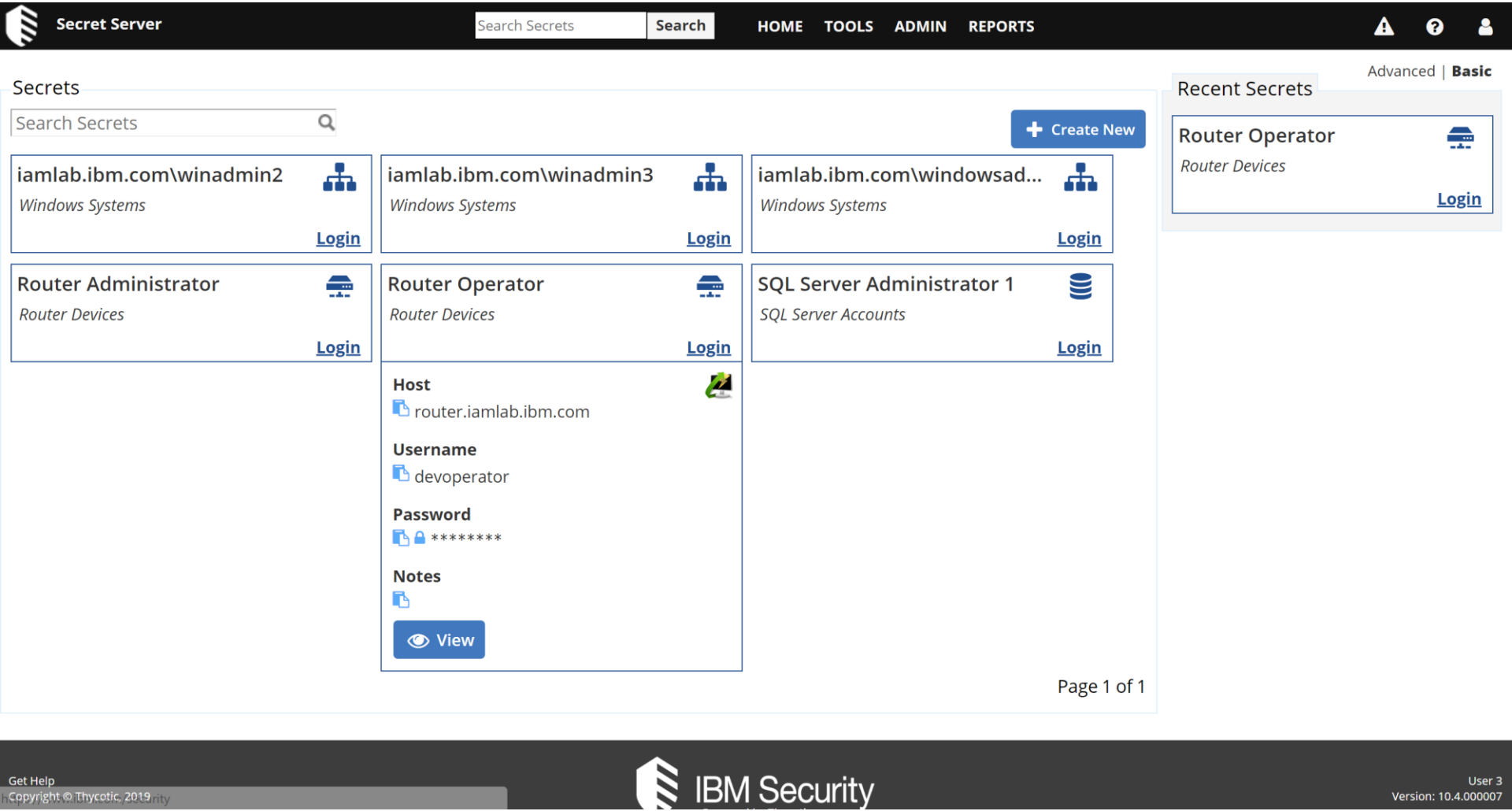
Elapsed	Type	Activity	Jump To
00:01:40		chrome	
00:01:40		chrome	
00:01:40		chrome	
00:01:40		chrome	
00:01:41		chrome	
00:01:41		chrome	
00:01:41		chrome	
00:01:41		chrome	
00:01:55		RuntimeBroker	
00:01:55		chrome	
00:01:56		chrome	
00:01:56		RuntimeBroker	
00:01:57		chrome	

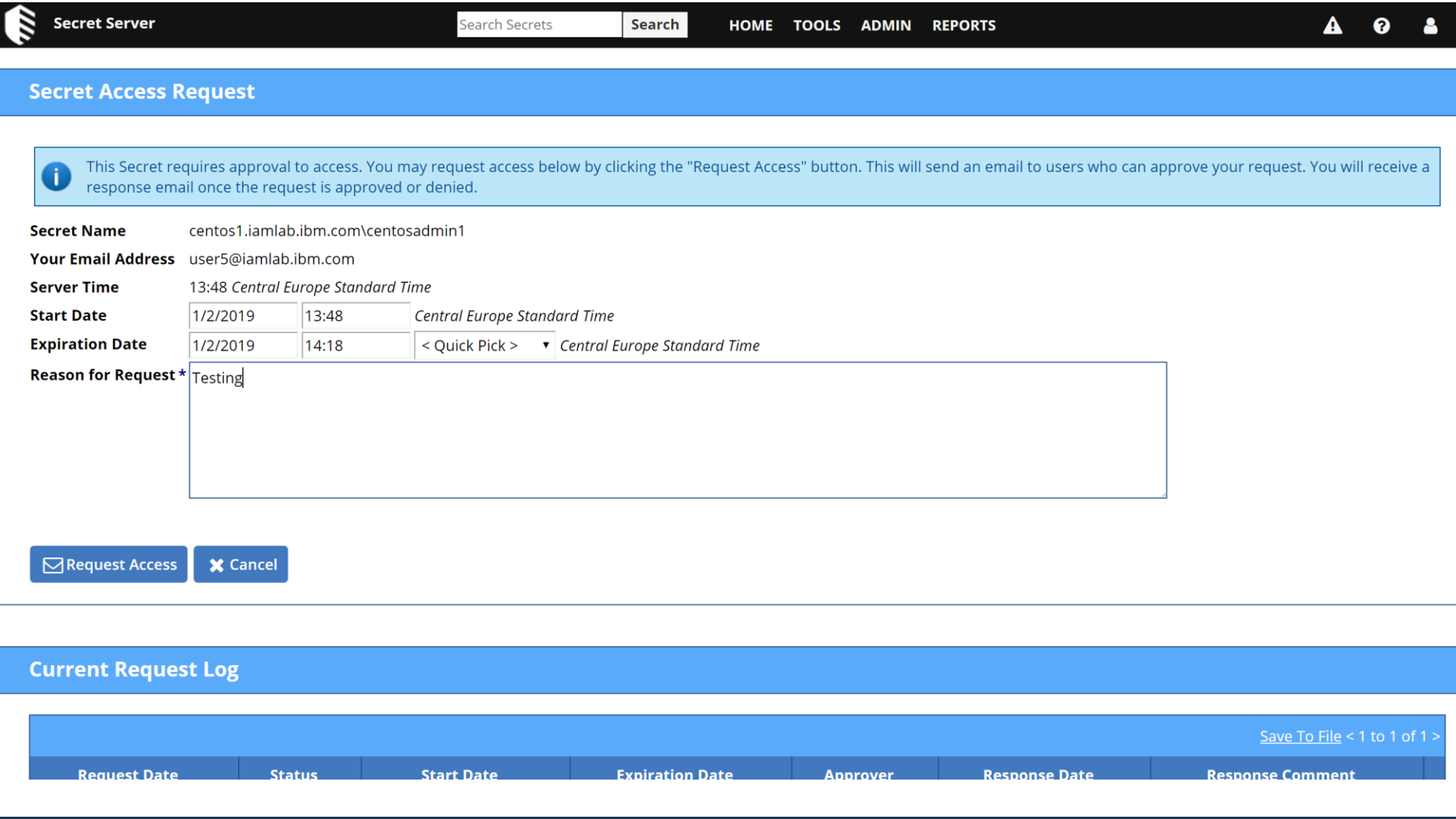


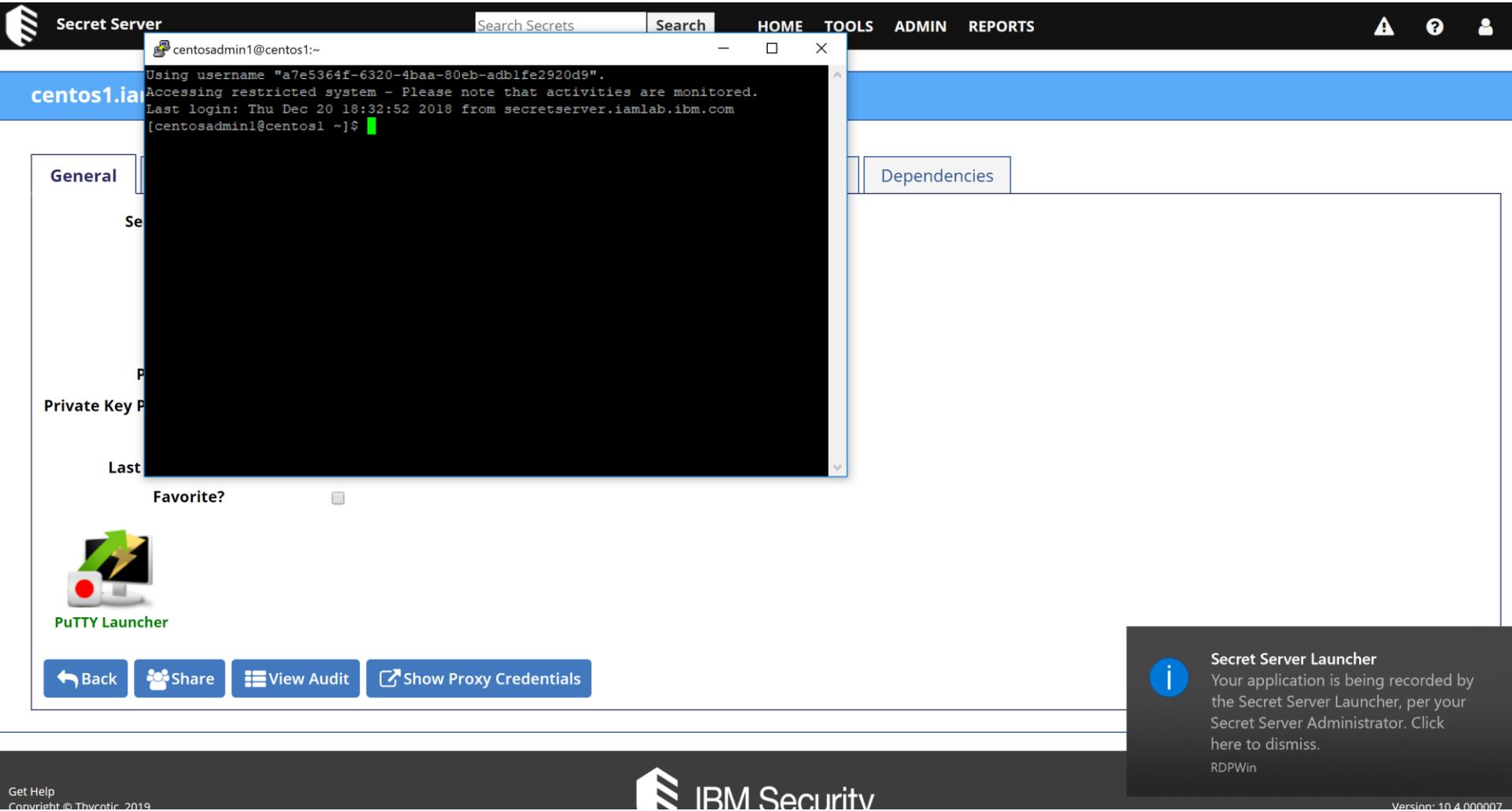
0:11:55 / 0:12:12

Screen
Keystrokes
Processes


Secret Server
Search Secrets
Search
HOME
TOOLS
ADMIN
REPORTS
3
An update is available (10.5.000003)
Reports
General
Security Hardening
User Audit
Secrets
What file types have been uploaded to Secrets?
What file types have been uploaded to Secrets? (Pie Chart)
What Secrets can all users see?
What Secrets can a user see?
What Secrets have been accessed?
What Secrets have been accessed by a user?
What Secret permissions exist?
What Secret permissions exist for a user?
What Secrets changed passwords in the last 90 days?
What Secrets have not changed passwords for over 90 days?
What Secret permissions exist for a group?
What Secrets don't require approval?
What Secrets have failed Heartbeat?
What Secrets require approval?
Secret Count per Site
What Secrets Do Not Have Distributed Engines?
What Secrets require Comments?
What Secrets have been accessed by an impersonated user?
What Secrets are expiring this week?
What Secrets Have Distributed Engines?
What Secrets have Expiration?
Secret Permissions Mismatch.
User
Failed login attempts
Who hasn't logged in within the last 90 days?
What SSH Command Menus do users have access to?
Secret Template Permissions by User
What users have had an admin reset their password?
Groups
Group Membership
Group Membership By Group
Roles and Permissions
What role permissions does a user have?
What role assignments exist?
What role permission assignments exist?
Password Compliance
Secret Password Compliance Statuses
What Secrets Do Not Meet Password Requirements?
Secret Policy
Activity
Secret Activity
Secret Activity Today
Secret Activity Yesterday
Folder Activity
Users Activity
Custom Report Activity
Dual Control Audit
Internal Communication Changes
IP Address Range Audit
Unlimited Administrator behavior
License Audit
Database Configuration Audit
Distributed Engine Activity
Event Subscription Activity
Secret Template Activity
Legacy Reports
Secret Server Usage
Secret Expiration Health
Secret Template Distribution
Top Ten Viewers
Discovery Scan


Secret Server
Search Secrets
Search
HOME
TOOLS
ADMIN
REPORTS
Advanced | Basic
Secrets
Search Secrets
Create New
iamlab.ibm.com\winadmin2
Windows Systems
Login
iamlab.ibm.com\winadmin3
Windows Systems
Login
iamlab.ibm.com\windowsad...
Windows Systems
Login
Router Administrator
Router Devices
Login
Router Operator
Router Devices
Login
SQL Server Administrator 1
SQL Server Accounts
Login
Host
router.iamlab.ibm.com
Username
devoperator
Password
****
Notes
View
Page 1 of 1
Recent Secrets
Router Operator
Router Devices
Login
Get Help
Copyright © Thycotic, 2019
IBM Security
User 3
Version: 10.4.000007

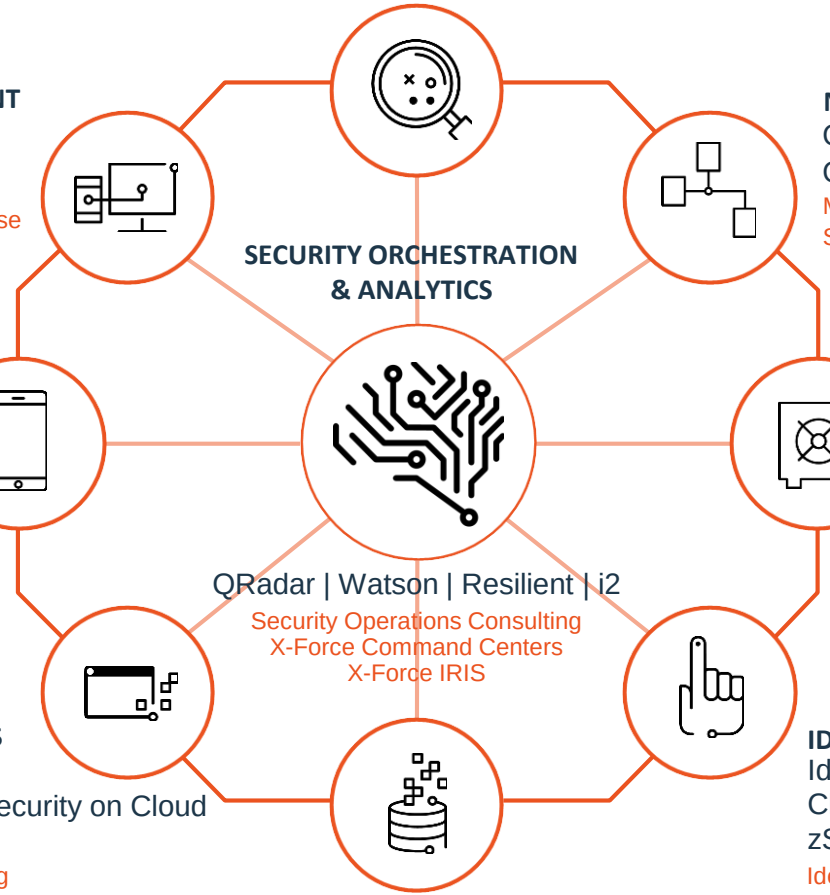

Secret Server
Search Secrets
Search
HOME
TOOLS
ADMIN
REPORTS
Secret Access Request
This Secret requires approval to access. You may request access below by clicking the "Request Access" button. This will send an email to users who can approve your request. You will receive a response email once the request is approved or denied.
Secret Name
centos1.iamlab.ibm.com\centosadmin1
Your Email Address
user5@iamlab.ibm.com
Server Time
13:48 Central Europe Standard Time
Start Date
1/2/2019
13:48
Central Europe Standard Time
Expiration Date
1/2/2019
14:18
< Quick Pick >
Central Europe Standard Time
Reason for Request *
Testing
Request Access
Cancel
Current Request Log
Save To File
< 1 to 1 of 1 >
Request Date
Status
Start Date
Expiration Date
Approver
Response Date
Response Comment


Secret Server
Search Secrets
Search
HOME
TOOLS
ADMIN
REPORTS
centosadmin1@centos1:~
Using username "a7e5364f-6320-4baa-80eb-adblfe2920d9".
Accessing restricted system - Please note that activities are monitored.
Last login: Thu Dec 20 18:32:52 2018 from secretserver.iamlab.ibm.com
[centosadmin1@centos1 ~]$
centos1.ia
General
Dependencies
Private Key P
Last
Favorite?
PuTTY Launcher
Back
Share
View Audit
Show Proxy Credentials
Secret Server Launcher
Your application is being recorded by the Secret Server Launcher, per your Secret Server Administrator. Click here to dismiss.
RDPWin
Get Help
IBM Security

ON PREM | CLOUD | HYBRID

THREAT INTELLIGENCE
X-Force Exchange | Malware Analysis
X-Force IRIS

SECURITY ECOSYSTEM
App Exchange
Hybrid Cloud Security Services



ENDPOINT
BigFix
Managed
Detection
& Response

NETWORK
QRadar Incident Forensics
QRadar Network Insights
Managed Network Security
Secure SD-WAN

MOBILE
MaaS360
Mobile Device Man

ADVANCED FRAUD
Trusteer
Financial Malware
Research

APPLICATIONS
AppScan
Application Security on Cloud
X-Force Red
SDLC Consulting

IDENTITY & ACCESS
Identity Governance and Access
Cloud Identity
zSecure
Identity Management Services

DATA
Guardium | Multi-cloud Encryption | Key Manager
Critical Data Protection Services

Products
Services

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM