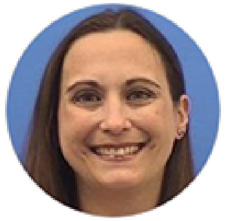
UIDPCONNECT
2021

RISE: A Secured Research Information Environment to Support U-I Collaboration

September 13, 2021 | 5:30 - 6:30 PM ET



Moderator:
Liv Blackmon
MITRE

Cheryl Doerr
Kansas State University

Jeremy Jackson
Anneal Initiative

Paul Lowe
Kansas State University

Danny Sewell
Kansas State University

Amy Billinger
Anneal Initiative

UIDP
Strengthening
University-Industry
Partnerships

RISE: A Secured Research Information Environment to Support University-Industry Collaboration

UIDPConnect 2021

Agenda

1. Background
2. Solution walkthrough
3. The Business Case/Application
4. Next steps
5. Questions

Controlled Unclassified Information (CUI)

Information provided by, collected, or maintained on behalf of, the executive branch of the United States government, and aligns with at least one of the CUI Registry categories.

Executive Order 13556

- Order establishes a program for managing CUI that emphasizes the openness and uniformity of Government-wide practice
- Established on 11/4/2010 under the 44th Administration

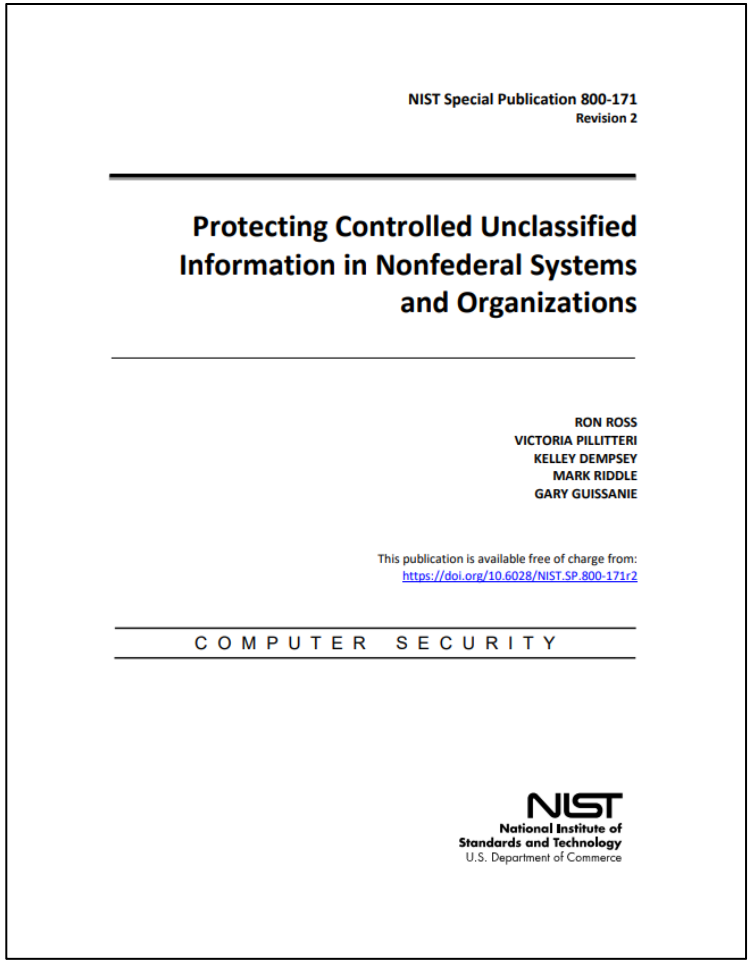
CUI Registry examples

- Export Control
- Intelligence
  - Agriculture
- Natural and Cultural Resources
- Nuclear
- Privacy
  - Student Records
- Transportation

NIST 800-171

Control Families

3.1 Access Control (22)
3.2 Awareness and Training (3)
3.3 Audit and Accountability (9)
3.4 Configuration Management (9)
3.5 Identification and Authentication (11)
3.6 Incident Response (3)
3.7 Maintenance (6)
3.8 Media Protection (9)
3.9 Personnel Security (2)
3.10 Physical Protection (6)
3.11 Risk Assessment (3)
3.12 Security Assessment (4)
3.13 System and Communications Protection (16)
3.14 System and Information Integrity (7)



NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Impact to K-State (Research)

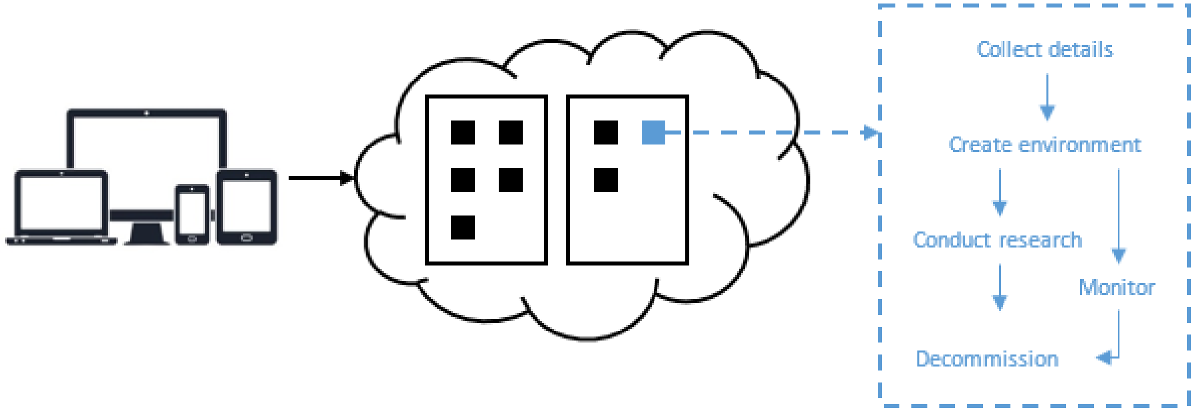
Very real risk to federally sponsored research

- ~33% of K-State portfolio

How do meet these new requirements

- Perform a readiness review with Anneal Initiative
- Formal self-assessment
- Isolate CUI with Microsoft Azure
- Research Information Security Enclave (RISE)

What is the application for university-industry collaboration?



CMMC for Universities and Industry

- Certification timelines unclear
  - Pilot/Pathfinder contracts and certification
- Compliance does not equal security (cyber or info)
  - Need an approach that accomplishes both
- Focus resources to protect covered info
  - Isolate from business or other networks
  - Limit access to those working covered projects
  - Support an awareness and security culture
- If it is not in writing it does not count
  - Planning, policies, procedures, and standards
- Ready access to objective evidence (for certification)

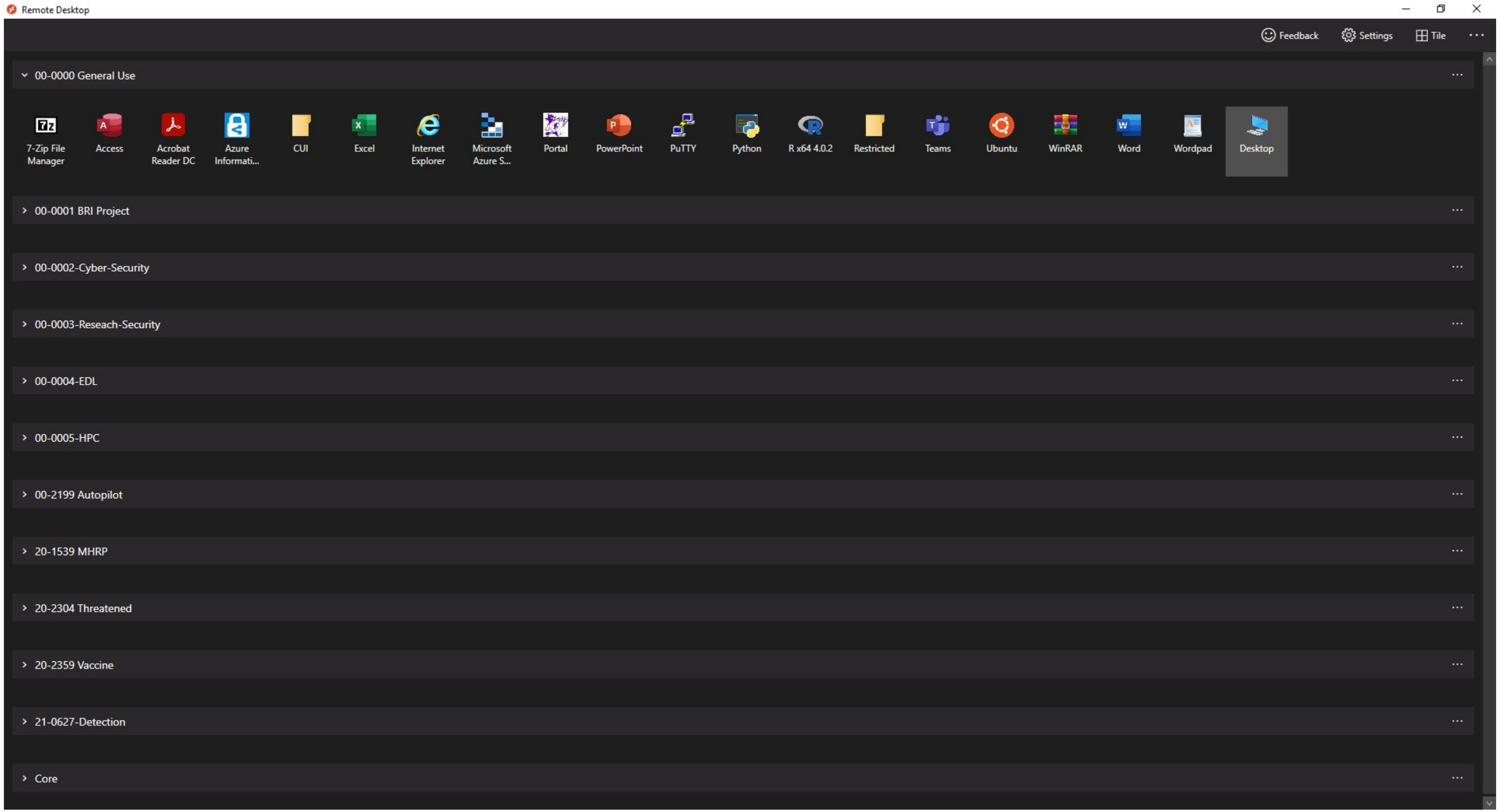
NIST/CMMC Challenges for Industry

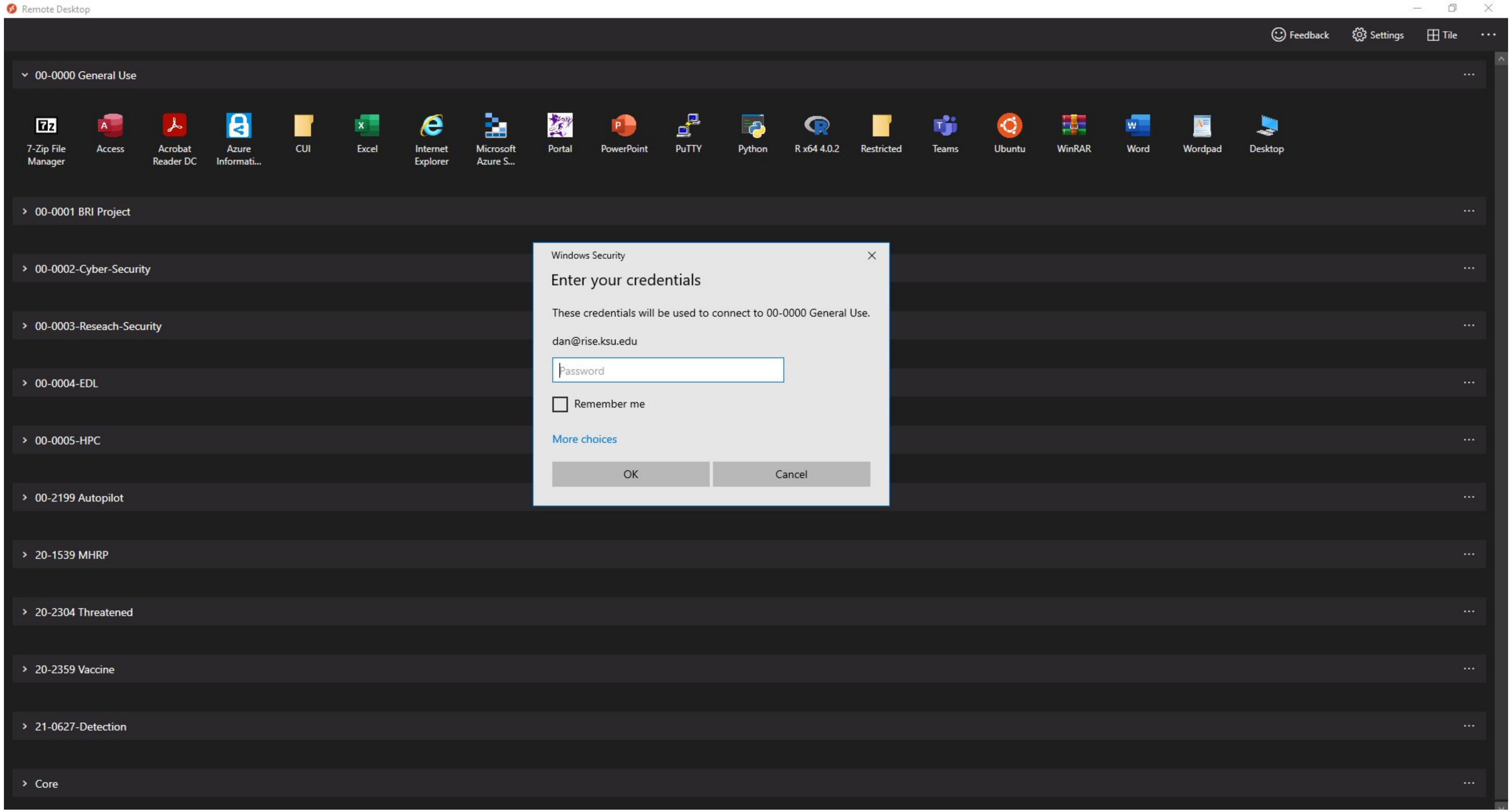
- Steep threshold to entry
  - Minimum seats with critical services
  - Cost of SIEMs, MFA, AD, encryption, authorized cloud services
  - Planning, policy, management and maintenance
  - **Certification** – moving target, unknown costs
- Information security is seen as an IT problem
- IT staffs are task saturated
- Not all MSPs/MSSPs are familiar/prepared
- Making cost allowable does not help competitiveness

Benefits of Third-Party Support

- Time- extensive effort & shifting environment
- Dedicated experts – get the support of a team
- Objective- independent; not influenced by hierarchy or politics
- More eyes- different perspective on security posture than MSP/IT Staff
- Ongoing Risk Analysis- threats, vulnerabilities, technology, and *regulations* change
- Planning and policy development- bridge gaps between CMMC and other organization efforts

Let’s see it


Remote Desktop
Feedback
Settings
Tile
00-0000 General Use
7-Zip File Manager
Access
Acrobat Reader DC
Azure Informati...
CUI
Excel
Internet Explorer
Microsoft Azure S...
Portal
PowerPoint
PuTTY
Python
R x64 4.0.2
Restricted
Teams
Ubuntu
WinRAR
Word
Wordpad
Desktop
00-0001 BRI Project
00-0002-Cyber-Security
00-0003-Reseach-Security
00-0004-EDL
00-0005-HPC
00-2199 Autopilot
20-1539 MHRP
20-2304 Threatened
20-2359 Vaccine
21-0627-Detection
Core



Windows Security

Enter your credentials

These credentials will be used to connect to 00-0000 General Use.

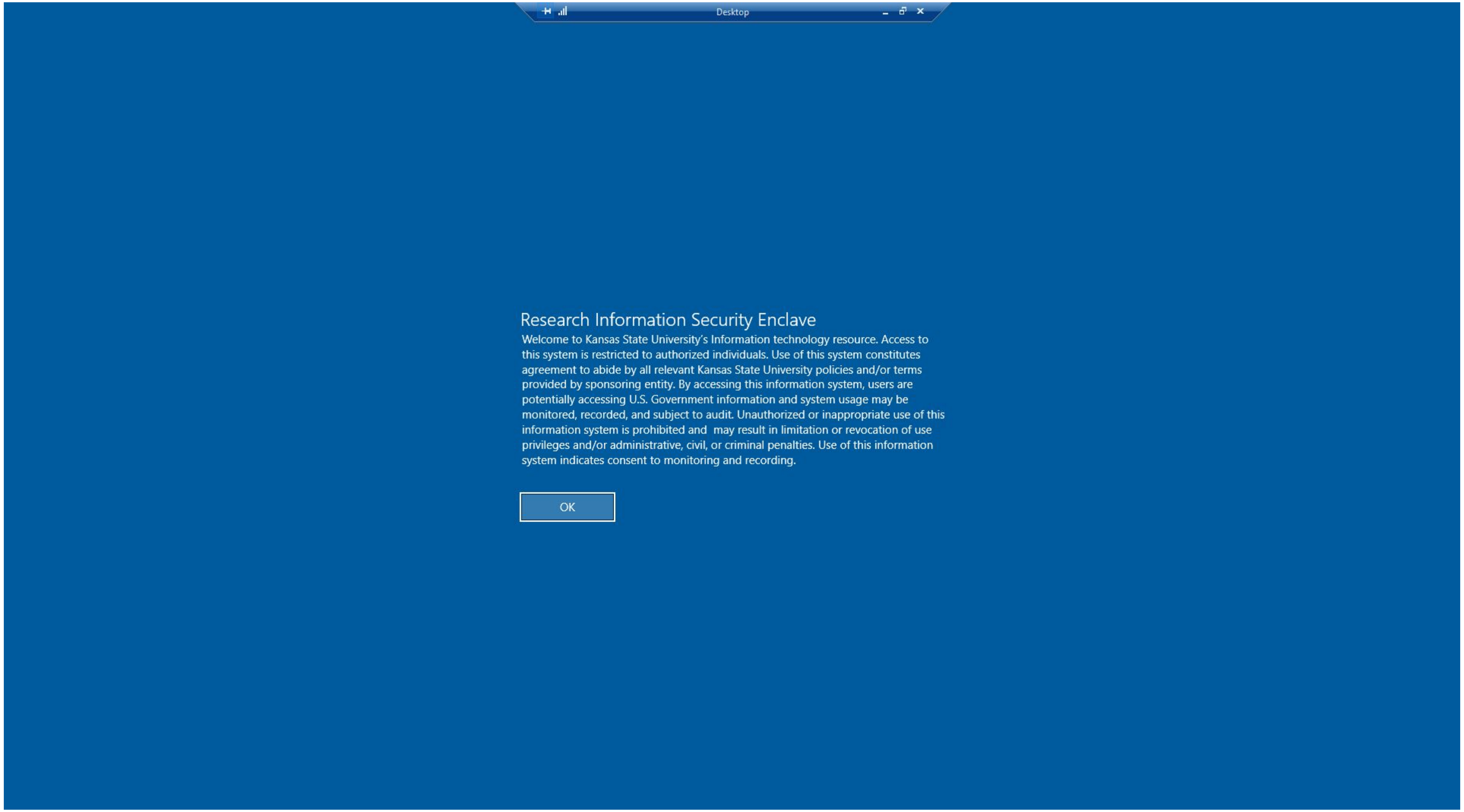
dan@rise.ksu.edu

Password

□ Remember me

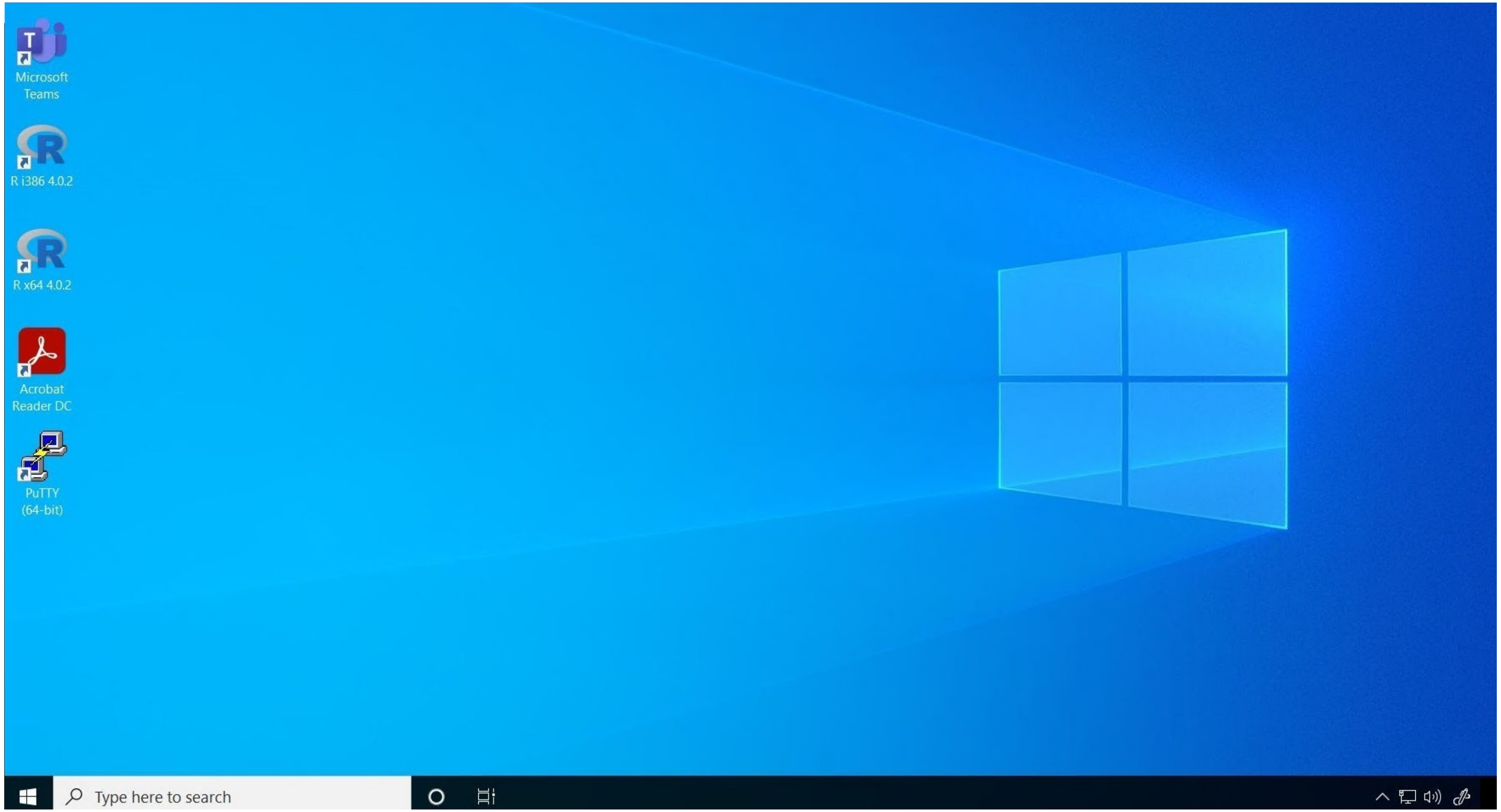
More choices

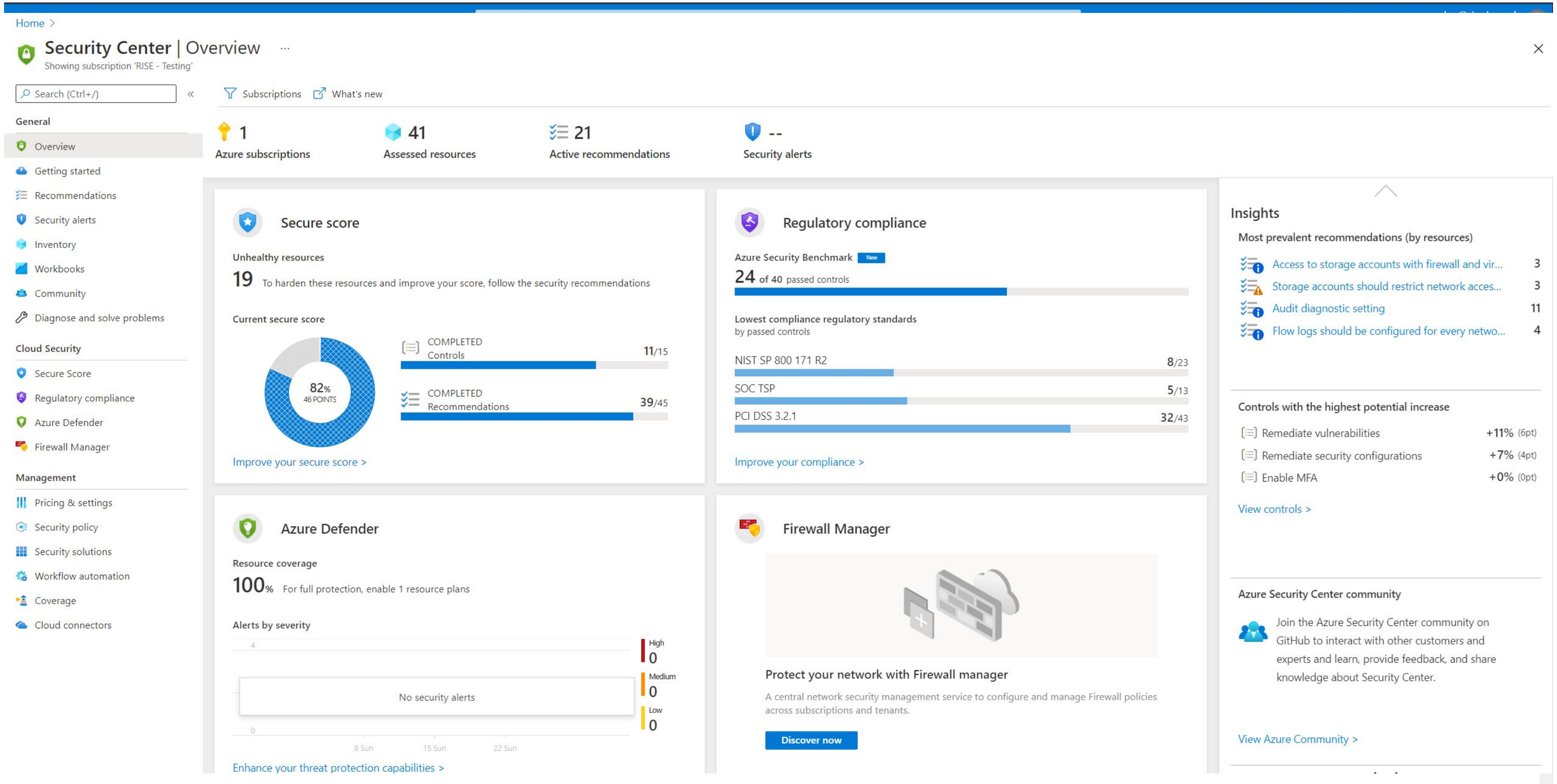
OK Cancel



Research Information Security Enclave

Welcome to Kansas State University's Information technology resource. Access to this system is restricted to authorized individuals. Use of this system constitutes agreement to abide by all relevant Kansas State University policies and/or terms provided by sponsoring entity. By accessing this information system, users are potentially accessing U.S. Government information and system usage may be monitored, recorded, and subject to audit. Unauthorized or inappropriate use of this information system is prohibited and may result in limitation or revocation of use privileges and/or administrative, civil, or criminal penalties. Use of this information system indicates consent to monitoring and recording.


Microsoft Teams
R i386 4.0.2
R x64 4.0.2
Acrobat Reader DC
PuTTY (64-bit)
Type here to search



Home >

Security Center | Overview ...

Showing subscription 'RISE - Testing'

Search (Ctrl+/) «

Subscriptions | What's new

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Secure Score
- Regulatory compliance
- Azure Defender
- Firewall Manager

Management

- Pricing & settings
- Security policy
- Security solutions
- Workflow automation
- Coverage
- Cloud connectors

1	41	21	--
Azure subscriptions	Assessed resources	Active recommendations	Security alerts

Secure score

Unhealthy resources

19 To harden these resources and improve your score, follow the security recommendations

Current secure score

82% 46 POINTS

COMPLETED Controls	11/15
COMPLETED Recommendations	39/45

Improve your secure score >

Regulatory compliance

Azure Security Benchmark New

24 of 40 passed controls

Lowest compliance regulatory standards by passed controls

NIST SP 800 171 R2	8/23
SOC TSP	5/13
PCI DSS 3.2.1	32/43

Improve your compliance >

Insights

Most prevalent recommendations (by resources)

Access to storage accounts with firewall and vir...	3
Storage accounts should restrict network acces...	3
Audit diagnostic setting	11
Flow logs should be configured for every netwo...	4

Controls with the highest potential increase

Remediate vulnerabilities	+11% (6pt)
Remediate security configurations	+7% (4pt)
Enable MFA	+0% (0pt)

View controls >

Azure Security Center community

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center.

View Azure Community >

Azure Defender

Resource coverage

100% For full protection, enable 1 resource plans

Alerts by severity

No security alerts

High	0
Medium	0
Low	0

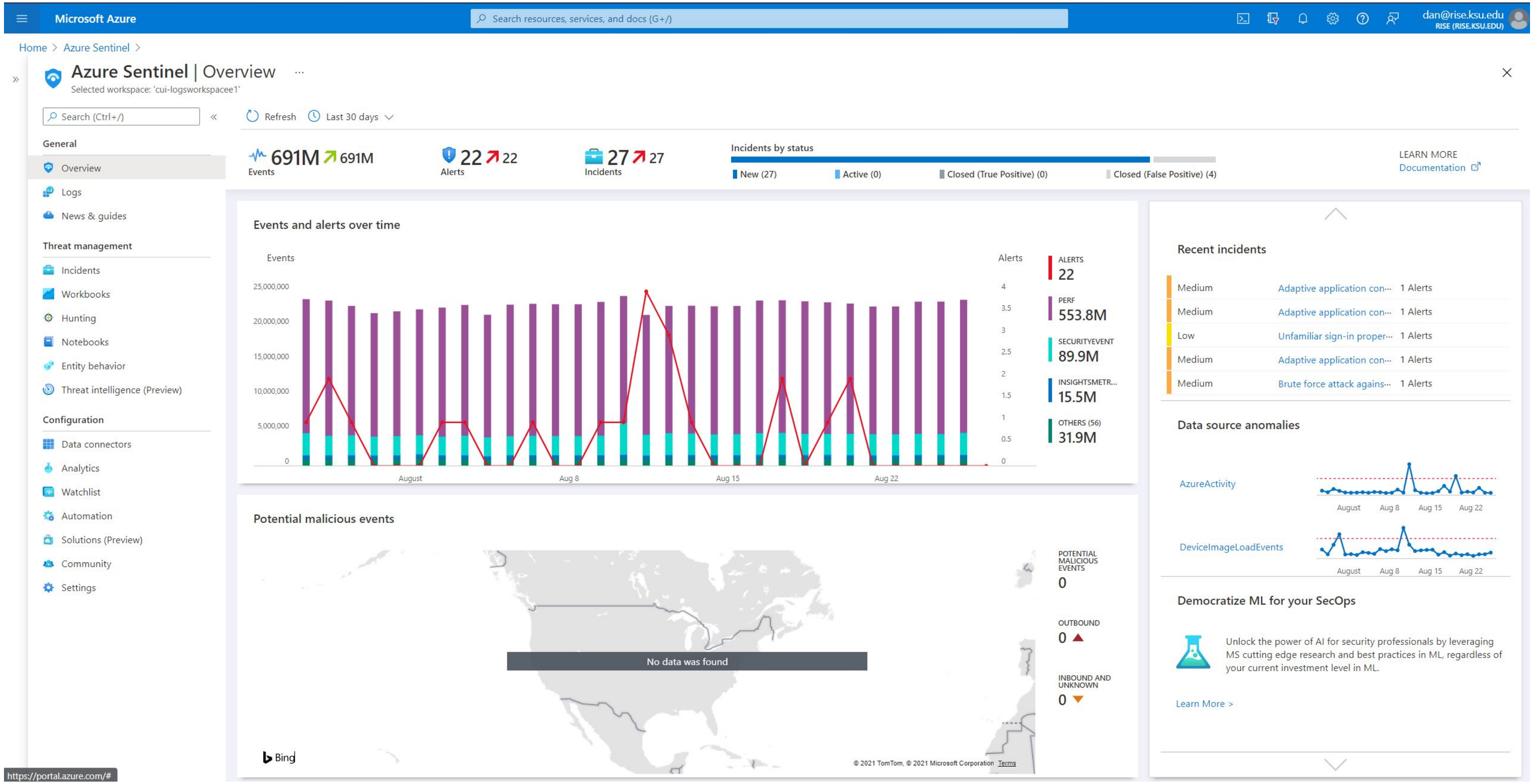
Enhance your threat protection capabilities >

Firewall Manager

Protect your network with Firewall manager

A central network security management service to configure and manage Firewall policies across subscriptions and tenants.

Discover now



Microsoft Azure

Search resources, services, and docs (G+/)

dan@rise.ksu.edu
RISE (RISE.KSU.EDU)

Home > Azure Sentinel >

Azure Sentinel | Overview

Selected workspace: 'cui-logsworkspacee1'

Search (Ctrl+/)

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist
- Automation
- Solutions (Preview)
- Community
- Settings

Refresh | Last 30 days

691M ↗ 691M
Events

22 ↗ 22
Alerts

27 ↗ 27
Incidents

Incidents by status

New (27) | Active (0) | Closed (True Positive) (0) | Closed (False Positive) (4)

LEARN MORE
Documentation

Events and alerts over time

ALERTS	22
PERF	553.8M
SECURITYEVENT	89.9M
INSIGHTSMETR...	15.5M
OTHERS (56)	31.9M

Potential malicious events

No data was found

POTENTIAL MALICIOUS EVENTS
0

OUTBOUND
0 ▲

INBOUND AND UNKNOWN
0 ▼

Recent incidents

Medium	Adaptive application con···	1 Alerts
Medium	Adaptive application con···	1 Alerts
Low	Unfamiliar sign-in proper···	1 Alerts
Medium	Adaptive application con···	1 Alerts
Medium	Brute force attack agains···	1 Alerts

Data source anomalies

AzureActivity

DeviceImageLoadEvents

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

Learn More >

https://portal.azure.com/#

What’s to come for K-State

- Additional standards
  - NIST SP 800-53 r5
  - NIST SP 800-172
  - DOD CMMC Level 3
  - “General research”

Any specific industry security needs not covered?

By leveraging the Microsoft Azure cloud (“Azure”), RISE meets the technical information security requirements established by the federal government. In addition, this solution may be deployed to facilitate a secure environment for the working with, sharing and storage of highly sensitive and proprietary information and data exchanged or generated through university-industry research collaborations.

RISE is intended to not only support an institution’s ability to meet multiple information security standards, but also to provide a path of least resistance for the research community, thus, fostering adoption of the RISE solution and alleviating the burden of information security from the research team.

Questions