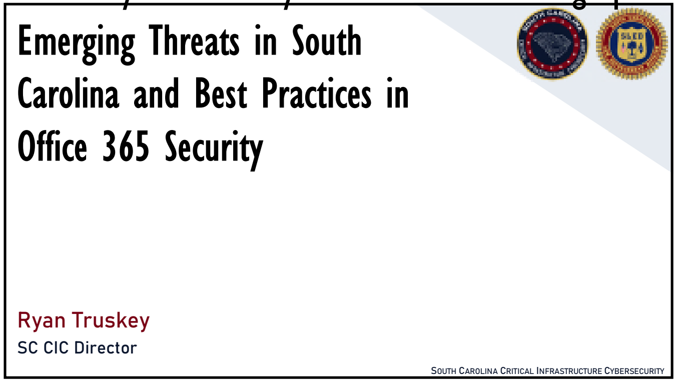
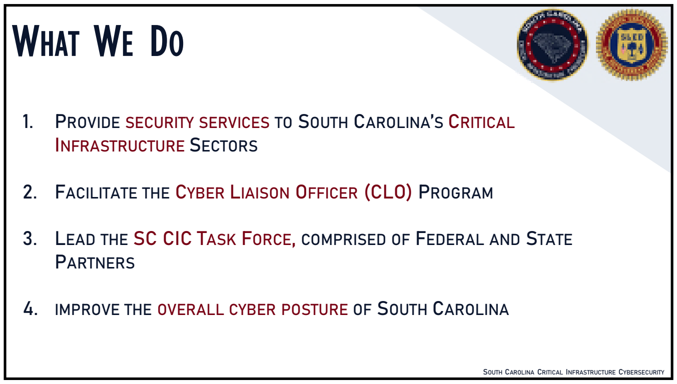
The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina.
Consult your attorney for advice concerning specific situations.



Emerging Threats in South Carolina and Best Practices in Office 365 Security

Ryan Truskey
SC CIC Director

South Carolina Critical Infrastructure Cybersecurity



What We Do

1. Provide security services to South Carolina's Critical Infrastructure Sectors
2. Facilitate the Cyber Liaison Officer (CLO) Program
3. Lead the SC CIC Task Force, comprised of Federal and State Partners
4. improve the overall cyber posture of South Carolina

South Carolina Critical Infrastructure Cybersecurity

SC CIC Task Force

SC Emergency Management Division
Cyber Incident Consequence Management

SC Election Commission
Election and Voter Information Security

SC Law Enforcement Division
Oversees the SC CIC Program

SC National Guard
125th Cyber Protection Battalion

SC Department of Administration
Division of Information Security

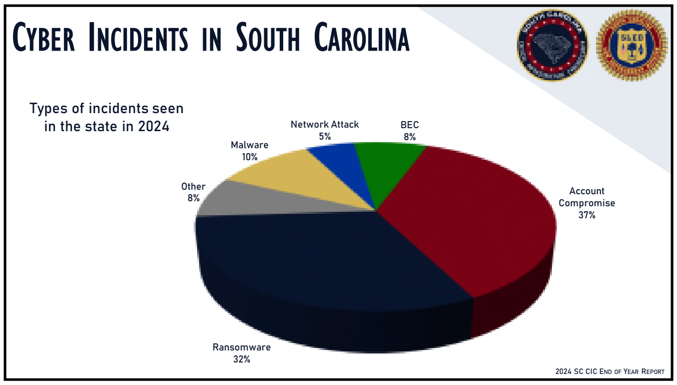
US Secret Service
Cyber Fraud Task Force

US Department of Homeland Security
Office of Intelligence and Analysis

US Department of Homeland Security
Cybersecurity & Infrastructure Agency

Federal Bureau of Investigations
Cyber Squad

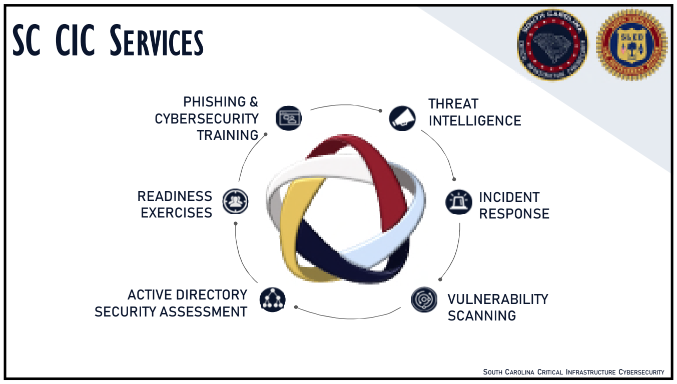
South Carolina Critical Infrastructure Cybersecurity



Cyber Incidents in South Carolina

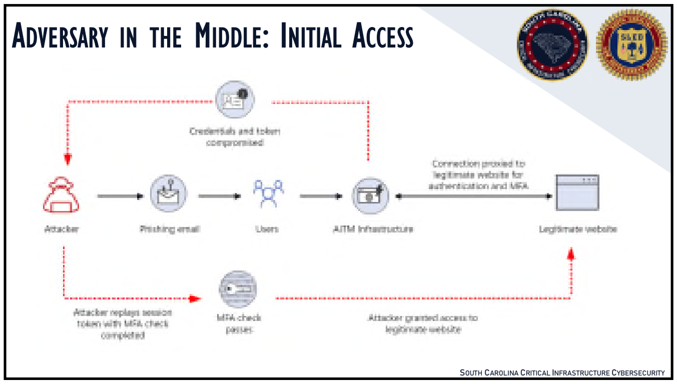
Types of incidents seen in the state in 2024

2024 SC CIC End of Year Report



SC CIC Services

South Carolina Critical Infrastructure Cybersecurity

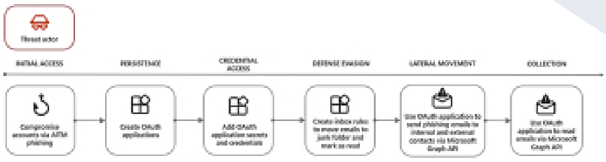


Adversary in the Middle: Initial Access

Credentials and token compromised
Connection proxied to legitimate website for authentication and MFA
Attacker
Phishing email
Users
AITM Infrastructure
Legitimate website
Attacker replays session token with MFA check completed
MFA check passes
Attacker granted access to legitimate website

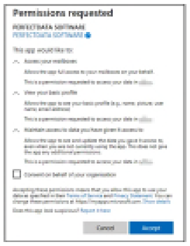
South Carolina Critical Infrastructure Cybersecurity

OAuth Abuse: Persistence & Others


Threat actor
INITIAL ACCESS
PERSISTENCE
CREDENTIAL ACCESS
DEFENSE EVASION
LATERAL MOVEMENT
COLLECTION
Compromise accounts via AiTM phishing
Create OAuth applications
Add OAuth application secrets and credentials
Create inbox rules to move emails to junk folder and mark as read
Use OAuth application to send phishing emails to internal and external contacts via Microsoft Graph API
Use OAuth application to read emails via Microsoft Graph API

South Carolina Critical Infrastructure Cybersecurity

OAuth Abuse: Persistence & Others



Permissions requested

PERFECTDATA SOFTWARE
PERFECTDATA SOFTWARE

This app would like to:

- Access your mailboxes
  Allows the app full access to your mailboxes on your behalf.
  This is a permission requested to access your data in [illegible].
- View your basic profile
  Allows the app to see your basic profile (e.g., name, picture, user name, email address)
  This is a permission requested to access your data in [illegible].
- Maintain access to data you have given it access to
  Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give the app any additional permissions.
  This is a permission requested to access your data in [illegible].

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

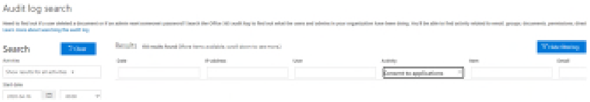
Does this app look suspicious? Report it here

39 organizations impacted in SC

South Carolina Critical Infrastructure Cybersecurity

OAuth Abuse: Persistence & Others

https://security.microsoft.com/auditlogsearch



Audit log search

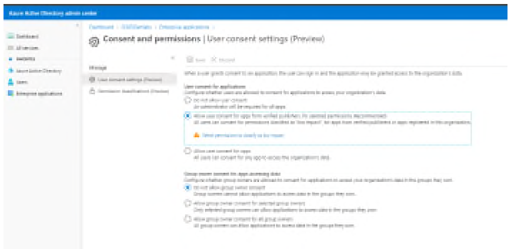
[illegible]

Activity: Consent to applications

Script to list all delegated permissions and application permissions in Microsoft Entra ID · GitHub

South Carolina Critical Infrastructure Cybersecurity

OAuth Abuse: Persistence & Others



Azure Active Directory admin center

Dashboard > [illegible] > Enterprise applications >

Consent and permissions | User consent settings (Preview)

Dashboard
All services
Favorites
Azure Active Directory
Users
Enterprise applications

Manage
User consent settings (Preview)
Permission classifications (Preview)

Save Discard

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data.

○ Do not allow user consent
An administrator will be required for all apps

● Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
Select permissions to classify as low impact

○ Allow user consent for apps
All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data
Configure whether group owners are allowed to consent for applications to access your organization's data in the groups they own.

● Do not allow group owner consent
Group owners cannot allow applications to access data in the groups they own.

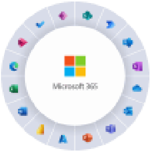
○ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data in the groups they own.

○ Allow group owner consent for all group owners
All group owners can allow applications to access data in the groups they own.

South Carolina Critical Infrastructure Cybersecurity

365 Best Practices

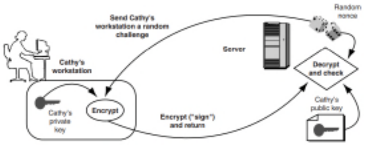
1. Implement phish-resistant multi-factor authentication (MFA)
2. Use conditional access policies
3. Utilize privileged identity management
4. Consider custom password ban list
5. Secure Microsoft Teams



South Carolina Critical Infrastructure Cybersecurity

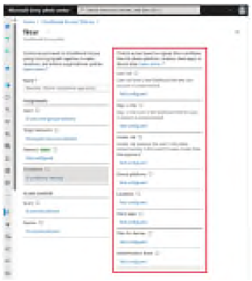
Phish-Resistant MFA

- FIDO2 Security Keys:
- Windows Hello For Business:
- Certificate-Based Authentication:



South Carolina Critical Infrastructure Cybersecurity

Conditional Access Policies



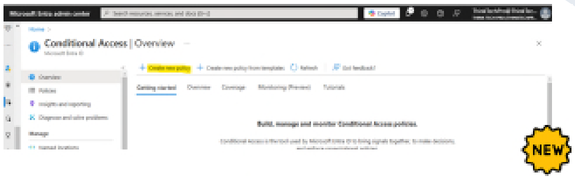
Top 3 recommended:

1) Azure AD Joined Devices
   Easier than ensuring compliance on every device

2) Restrict Access based on Location
   Factor in vendors, partners, and travel habits of employees to avoid business disruption

3) Block Unused Operating System
   Review and confirm OSs in environment prior to rolling out

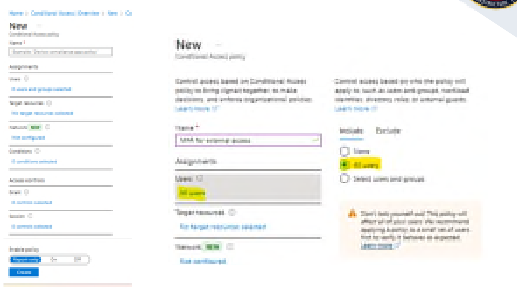
Conditional Access Policies



Conditional Access | Overview

Build, manage and monitor Conditional Access policies.

Conditional Access Policies



New
Conditional Access policy

Name *
MFA for external access

Assignments

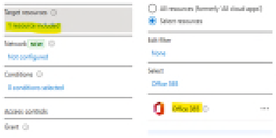
Users
All users

Target resources
No target resources selected

Network NEW
Not configured

○ None
● All users
○ Select users and groups

Conditional Access Policies



Target resources ⓘ

1 resource included

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

○ All resources (formerly 'All cloud apps')

● Select resources

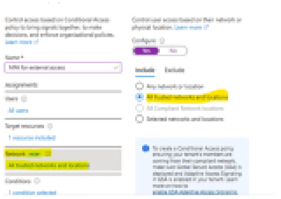
Edit filter

None

Select

Office 365

Office 365 ⓘ



Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

MFA for external access

Assignments

Users ⓘ

All users

Target resources ⓘ

1 resource included

Network NEW ⓘ

All trusted networks and locations

Conditions ⓘ

1 condition selected

Control user access based on their network or physical location. Learn more

Configure ⓘ

Yes No

Include Exclude

○ Any network or location

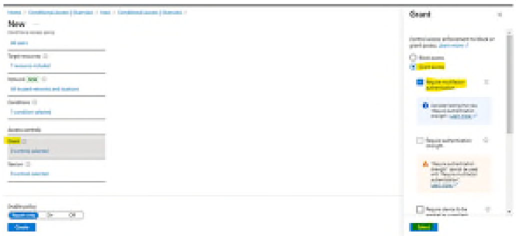
● All trusted networks and locations

○ All Compliant Network locations

○ Selected networks and locations

South Carolina Critical Infrastructure Cybersecurity

Conditional Access Policies



Home > Conditional Access | Overview > New > Conditional Access | Overview >

New

Conditional Access policy

All users

Target resources ⓘ

1 resource included

Network NEW ⓘ

All trusted networks and locations

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only On Off

Create

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multifactor authentication

□ Require authentication strength

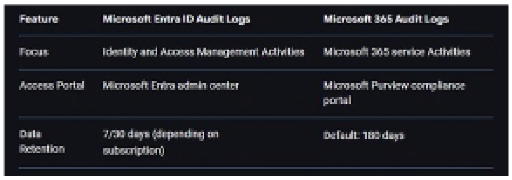
□ Require device to be marked as compliant

Select

South Carolina Critical Infrastructure Cybersecurity

Audit Logging And Alerting

Retention Policies



Feature	Microsoft Entra ID Audit Logs	Microsoft 365 Audit Logs
Focus	Identity and Access Management Activities	Microsoft 365 service Activities
Access Portal	Microsoft Entra admin center	Microsoft Purview compliance portal
Data Retention	7/30 days (depending on subscription)	Default: 180 days

South Carolina Critical Infrastructure Cybersecurity

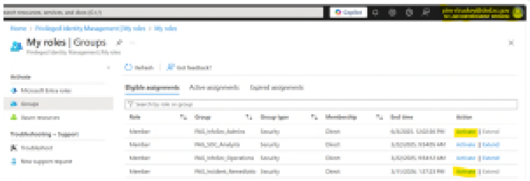
Privileged Identity Management (PIM)

Key Features:

- Provide just-in-time privileged access to Microsoft Entra ID and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce conditional access to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles

Microsoft Entra
ID P2

Privileged Identity Management (PIM)

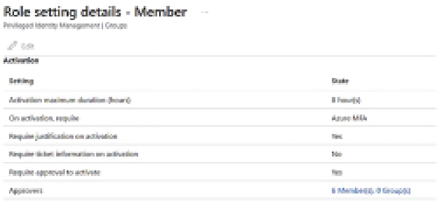


My roles | Groups

Privileged Identity Management | My roles

Role	Group	Group type	Membership	End time	Action
Member	PAG_Infosec_Admins	Security	Direct	6/3/2025, 12:02:56 PM	Activate | Extend
Member	PAG_SOC_Analysts	Security	Direct	3/20/2025, 9:34:05 AM	Activate | Extend
Member	PAG_Infosec_Operations	Security	Direct	3/20/2025, 9:54:17 AM	Activate | Extend
Member	PAG_Incident_Remediate	Security	Direct	3/11/2026, 1:27:23 PM	Activate | Extend

Privileged Identity Management (PIM)



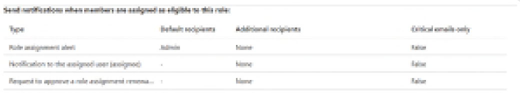
Role setting details - Member

Privileged Identity Management | Groups

Activation

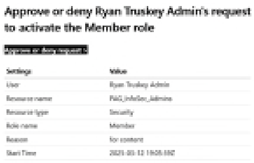
Setting	State
Activation maximum duration (hours)	8 Hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	6 Member(s), 0 Group(s)

Privileged Identity Management (PIM)



Send notifications when members are assigned as eligible to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	Admin	None	False
Notification to the assigned user (assignee)	-	None	False
Request to approve a role assignment renewa...	-	None	False



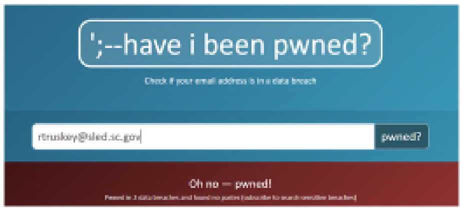
Approve or deny Ryan Truskey Admin's request to activate the Member role

Approve or deny request >

Settings	Value
User	Ryan Truskey Admin
Resource name	PAG_InfoSec_Admins
Resource type	Security
Role name	Member
Reason	for content
Start Time	2025-03-12 19:05 EDT

South Carolina Critical Infrastructure Cybersecurity

Custom Password Ban List



';--have i been pwned?

Check if your email address is in a data breach

rtruskey@sled.sc.gov

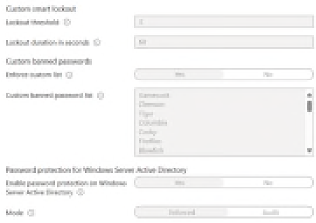
Oh no — pwned!

Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)

Microsoft Entra ID P1

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-deploy

Custom Password Ban List



Custom smart lockout

Lockout threshold: 3

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: Yes | No

Custom banned password list:

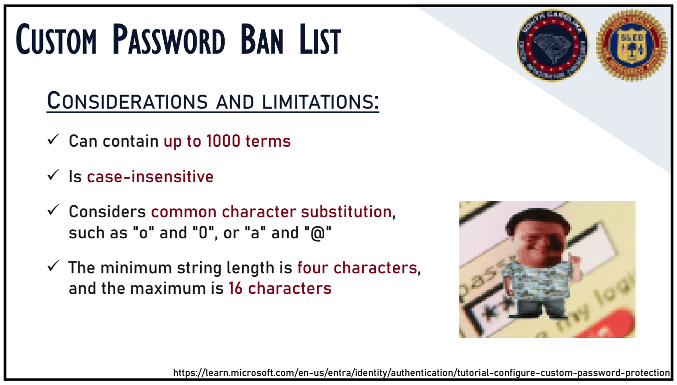
Gamecock
Clemson
Tiger
Columbia
Cocky
Fireflies
Blowfish

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes | No

Mode: Enforced | Audit

https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection

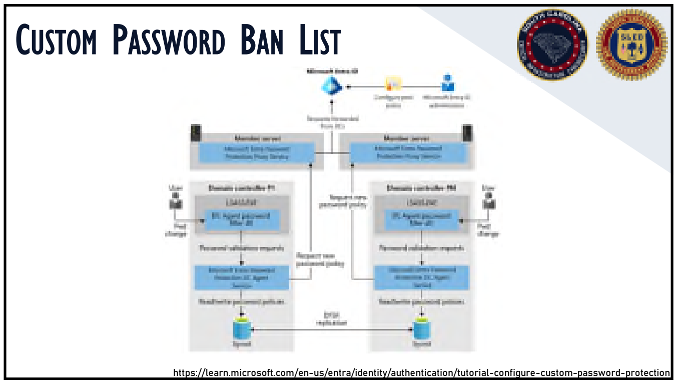


Custom Password Ban List

Considerations and limitations:

- ✓ Can contain up to 1000 terms
- ✓ Is case-insensitive
- ✓ Considers common character substitution, such as "o" and "0", or "a" and "@"
- ✓ The minimum string length is four characters, and the maximum is 16 characters

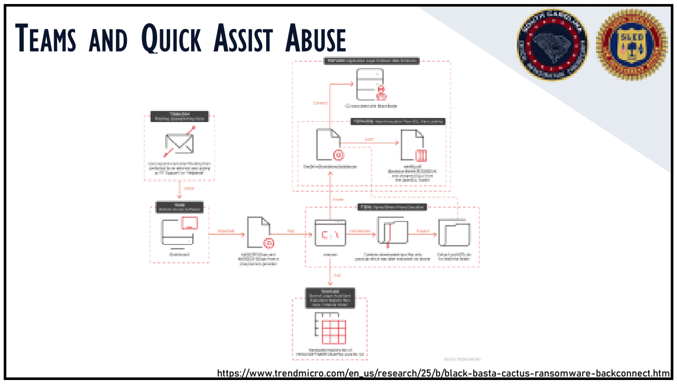
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection



Custom Password Ban List

Microsoft Entra ID
Configure ban policy
Microsoft Entra ID administrator
Requests forwarded from DCs
Member server
Microsoft Entra Password Protection Proxy Service
Member server
Microsoft Entra Password Protection Proxy Service
User
Pwd change
Domain controller #1
LSASS.EXE
DC Agent password filter dll
Password validation requests
Microsoft Entra Password Protection DC Agent Service
Read/write password policies
Sysvol
Request new password policy
Request new password policy
DFSR replication
Domain controller #N
LSASS.EXE
DC Agent password filter dll
Password validation requests
Microsoft Entra Password Protection DC Agent Service
Read/write password policies
Sysvol
User
Pwd change

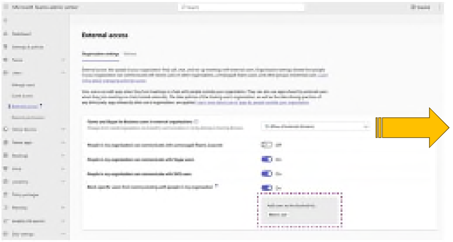
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection

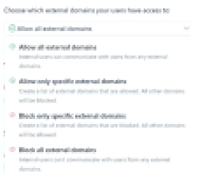


Teams and Quick Assist Abuse

https://www.trendmicro.com/en_us/research/25/b/black-basta-cactus-ransomware-backconnect.html

Teams Security


External access


Choose which external domains your users have access to

Allow all external domains

Allow all external domains
External users can communicate with users from any external domains.

Allow only specific external domains
Create a list of external domains that are allowed. All other domains will be blocked.

Block only specific external domains
Create a list of external domains that are blocked. All other domains will be allowed.

Block all external domains
External users can't communicate with users from any external domains.

HTTPS://LEARN.MICROSOFT.COM/EN-US/MICROSOFTTEAMS/TRUSTED-ORGANIZATIONS-EXTERNAL-MEETINGS-CHAT

Grants

South Carolina Critical Infrastructure Cybersecurity

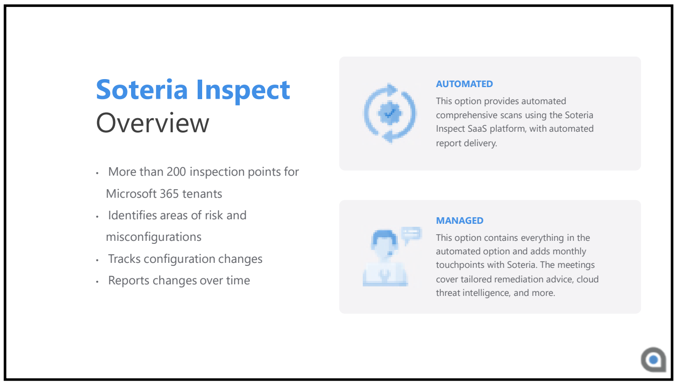
Grants

South Carolina	South Carolina Law Enforcement Division	Robert Connell (803) 896-7021 rconnell@sled.sc.gov

FEMA

The State Administrative Agency (SAA) is the only entity eligible to apply for and submit the application for the State and Local Cybersecurity Grant Program (SLCGP), Homeland Security Grant Program (HSGP) and its component programs.

South Carolina Critical Infrastructure Cybersecurity



Soteria Inspect
Overview

- More than 200 inspection points for Microsoft 365 tenants
- Identifies areas of risk and misconfigurations
- Tracks configuration changes
- Reports changes over time

AUTOMATED

This option provides automated comprehensive scans using the Soteria Inspect SaaS platform, with automated report delivery.

MANAGED

This option contains everything in the automated option and adds monthly touchpoints with Soteria. The meetings cover tailored remediation advice, cloud threat intelligence, and more.