2025
Year In Review

South Carolina Critical Infrastructure Cybersecurity

Table of Contents

Executive Summary

In 2025, South Carolina Critical Infrastructure Cybersecurity (SC CIC) expanded its reach, strengthened statewide cyber readiness, and deepened its proactive approach to protecting essential services. Through expedient intelligence sharing, hands-on preparedness efforts, and incident response support, SC CIC reinforced its role as a centralized cybersecurity partner for critical infrastructure organizations across the state.

2025 Program Highlights

+326
Participating organizations across 15 of 16 critical infrastructure sectors

2
SC CIC also hosted its second annual cybersecurity conference

608
Cyber Liaison Officers statewide, an increase of 123 CLOS from 2024

120
Cyber Liaison Officers attended the SC CIC cybersecurity conference

12
External Partners joined in response to the launch of the External Partner program

+40
Presentations and event facilitations participated in by SC CIC Staff

2025 Services Highlights

85
Significant cyber incidents

52
Active Directory (AD) assessments conducted

+2,500
Malware files and artifacts analyzed

22%
Average AD assessment score improvement

229
Organizations engaged in the threat intelligence program

63
Microsoft 365 security assessments performed in partnership with Soteria

+1,700
Leaked credentials were identified

~30
Phishing simulations facilitated

328
Malicious sites were taken down

173
Vulnerability scanning engagements

+193K
IP addresses monitored

+22K
Endpoints protected through SLCGP-funded CheckPoint EDR/MDR solution

807
Domains monitored

Looking Ahead

As SC CIC moves into 2026, there are several key initiatives that SC CIC is looking to implement.

- The first is to coordinate more in-person events for both technical training and networking for information security professionals and cybersecurity students across South Carolina.
- The second is to continue advancing the SC CIC team forward with the hiring of new positions, along with proactively training on relevant topics.
- The final initiative is to continue pursuing growth in both participating organizations and partnerships in both a statewide and national capacity.

Overview

South Carolina Critical Infrastructure Cybersecurity (SC CIC) was established in April 2017 by an executive order from South Carolina Governor Henry McMaster after gaps in cybersecurity support for critical infrastructure below the state level were identified. SC CIC's mission is to facilitate cybersecurity intelligence sharing and to improve the overall cybersecurity posture of South Carolina's critical infrastructure. SC CIC provides critical services to both public and private critical infrastructure organizations at no cost to them.

SC CIC services include threat intelligence, readiness exercises, Active Directory (AD) assessments, phishing and security awareness training, Microsoft 365 (M365) security assessments, and vulnerability scanning. These services have been implemented with the aim of making a significant impact and positively contributing to the improvement of South Carolina's cybersecurity posture. This is one of the many factors that makes SC CIC unique and preserves its relevancy. Rather than solely focusing on responding to significant cyber incidents, SC CIC aims to remain proactive and prevent such events from occurring. This document will provide an overview and statistical highlights of SC CIC's efforts to protect the South Carolina's critical infrastructure in 2025.

SC CIC Personnel

The strength of any great program is its people, and SC CIC is no different. Our team includes the program director, deputy director of security services, deputy director of program management, two cyber threat intelligence analysts, four analysts with complementing security specialties, a detection engineer, a security engineer, a cybersecurity advisor, and a program coordinator. These **thirteen team members** enable SC CIC to provide timely assistance to the state's critical infrastructure and consistently deliver exceptional results. Following the pattern of 2024, our team has obtained additional state funding, which will support expansion to better meet growing cybersecurity demands within the state. This expansion will allow the team to continue refining its services, reaching an even wider audience, and spend more time with each individual organization.

Ryan Truskey
SLED CIO,
SC CIC Director

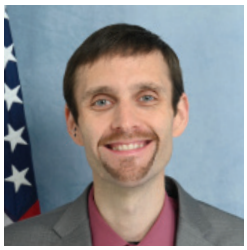
Lucas Cobb
Deputy Director—
Security Services

Lauren Barwick
Deputy Director—
Program Manager

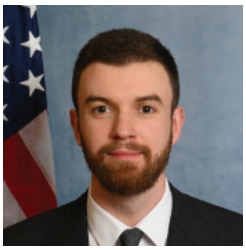
Tim Larkin
Cybersecurity
Advisor

Caitlin Scroggins
Program
Coordinator

Joshua McDill
Security Engineer



Matt Norris
Security Analyst



Stan Verchenko
Security Analyst

Sadie Slusher
Security Analyst

Joe Taylor
Security Analyst

Collin Lairamore
Threat Detection
Engineer

Ryan Cummings
Threat Intelligence
Analyst

Debon Grady
Threat Intelligence
Analyst

Program Growth

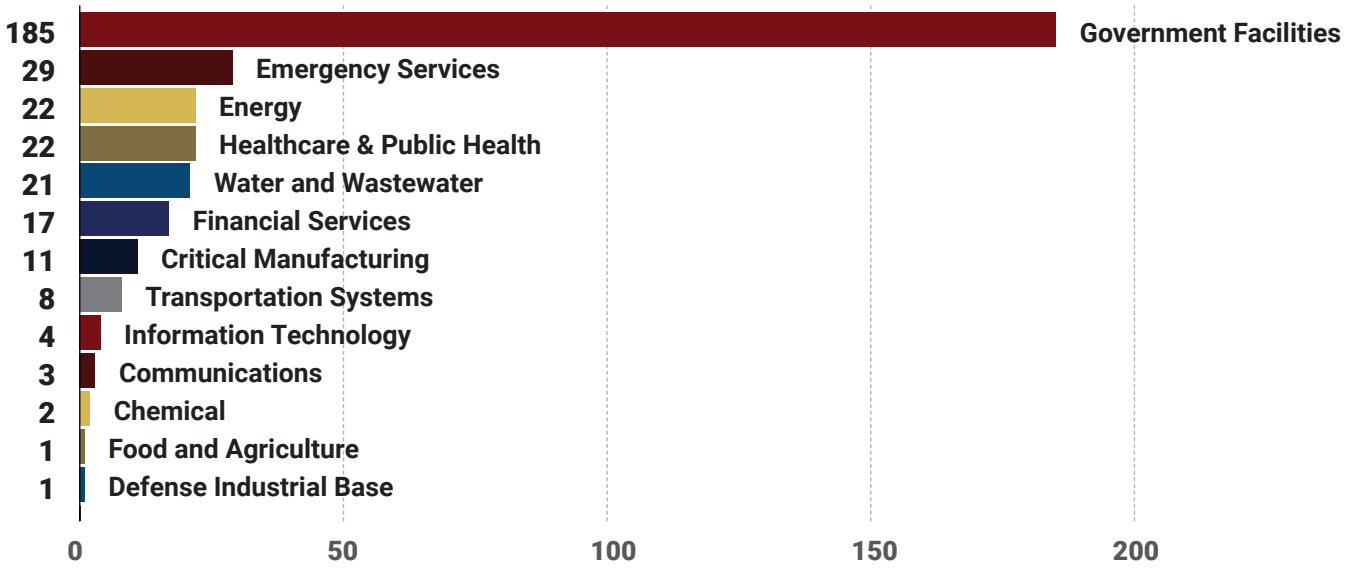
In 2025, the total number of SC CIC organizations grew to **326**, an increase by **47** from the previous year. These organizations represent **15 out of the 16 critical infrastructure sectors** identified by Presidential Policy Directive 21 (PPD-21)[1]. The sector not represented is Commercial Facilities. SC CIC services may be offered to this sector; however, due to a cyberattack being more likely to cause financial losses than disrupt essential services, requests continue to be evaluated on an individual basis. As with previous years, **Government Facilities remains the most represented sector in SC CIC**. Because of SC CIC's mission to serve critical infrastructure entities operating below the state level, this sector will always remain a primary focus. The considerable addition of new organizations and partnerships exemplifies the success of SC CIC's intentional focus on relationship building and networking across both South Carolina and the greater United States.

326
Total SC CIC Organizations

+47
New organizations

15
Critical Infrastructure Sectors

SC CIC Organizations by Sector



It should be noted that some organizations fall under multiple critical infrastructure sectors, so the number of sectors present in the SC CIC Organizations by Sector chart may differ from the number mentioned in the above text.

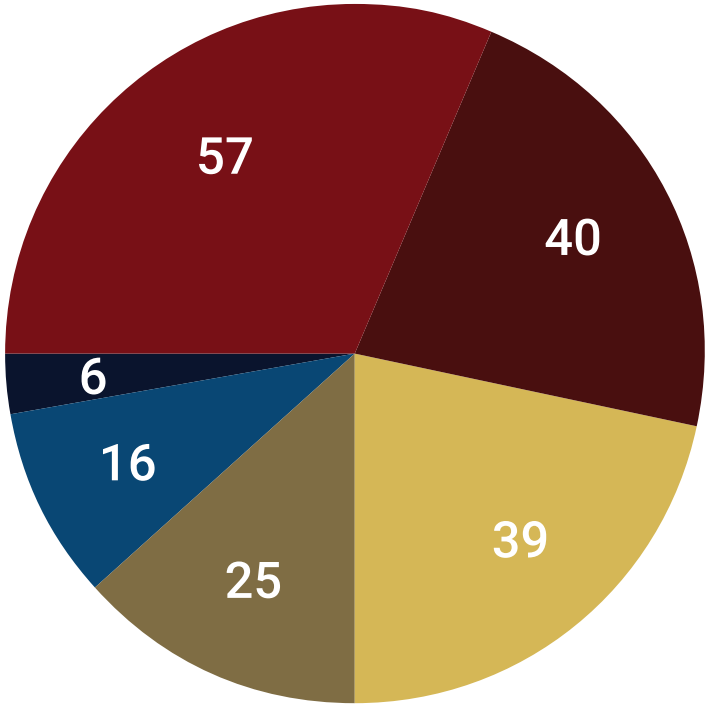
1 https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and

Government Facilities

The Government Facilities Sector is comprised of local and state government, in addition to the Education Facilities and Elections Infrastructure Subsectors. The following graph further categorizes the **183** organizations that fall under government facilities in SC CIC to help understand this sector's makeup. The **Education Facilities Subsector is the largest**, which includes private and public K-12 schools as well as public and private higher education institutions. The **County-Level Support** category represents agencies that operate at the county level, such as solicitor's offices.

Government Facilities Sector Breakdown

- **57 Education (K-12)**
- **40 City/Town**
- **39 County**
- **25 State Agency**
- **16 Education (Higher)**
- **6 County Support**



Cyber Liaison Officer Program

Cyber Liaison Officers (CLOs) are the integral foundation of SC CIC.

CLOs are IT professionals and administrators who coordinate their organization's onboarding into SC CIC, identify which services to engage in, and then participate in events to implement the knowledge obtained into their daily operations. CLOs serve as the primary point of contact, playing a crucial role in continuing the robust threat intelligence ecosystem created by SC CIC in South Carolina. The facilitation of two way information sharing allows cyber-related information, like cyber threats, incidents, and trends seen both in South Carolina and the greater world, to be disseminated in an expedient and efficient manner. **At the end of 2025, the total number of SC CIC CLOs was 608**, an increase of 123 from 2024.

608
Total CLOs

+123
New CLOs

SC CIC External Partners

In 2025, SC CIC launched a new participation initiative called "External Partners". External Partners were created with the mission of increasing cyber-related information sharing across South Carolina as well as facilitating partnerships with state associations and federal agencies that support critical infrastructure organizations in South Carolina. External partners play a critical role in broadening the reach of SC CIC by sharing pertinent threat intelligence and other cyber-related information to those who may not currently participate in SC CIC. Additionally, through these partnerships, SC CIC is able to gain sector specific perspectives regarding how we can continue to support their members as it relates to cybersecurity. At the end of 2025, there are **12 External Partners** who are actively engaged with SC CIC.

CLO Calls

SC CIC hosts monthly calls to facilitate communication and networking between participants and the team, along with providing timely and relevant updates. These calls cover the latest cyber threat intelligence, offering valuable insights into the dynamic cyber threat landscape in South Carolina and the wider world. This year's call highlights included:

- A discussion from **Infoblox** covering email mitigation, observed phishing trends, and the email takedown escalation process.
- **11 incident recaps and walk-throughs** presented by the SC CIC team.
- A deep dive into **ClickFix phishing trends** and **how to detect it** within your environment.
- **Ransomware trends** and **threat actors** observed both in South Carolina and the greater nation.

External Engagements

SC CIC participates in regular external engagements to facilitate and cultivate relationships with critical infrastructure stakeholders and other key partners. These opportunities foster invaluable information sharing with the security community and provides SC CIC critical insight into the state's current cybersecurity posture and challenges.

In 2025, SC CIC personnel were invited to participate in **40 events** including conferences, trainings and symposiums.

- The State of SC Cyber Symposium
- America's Credit Unions Cybersecurity Conference
- Security Awareness Trainings for five organizations across South Carolina
- The South Carolina School Board Insurance Trust (SCSBIT)'s annual Risky Business Conference
- South Carolina Association for Educational Technology (SCAET)'s annual EdTech Conference
- Municipal Technology Association of South Carolina (MTASC)'s Fall and Spring conferences
- The National Governor's Association

SC CIC Office Hours

SC CIC also hosts its own events throughout the year. Each month, informal meetings called SC CIC Office Hours are held, giving CLOs the opportunity to ask questions, network, and build relationships with other CLOs and External Partners from across the state. These are normally conducted virtually but periodically are held in-person at SC higher education institutions to promote networking. While no in-person events were facilitated in 2025, **SC CIC has prioritized partnering with higher education institutions across South Carolina in 2026 to continue forging strong connections with college graduates and their potential future employers in the state.**

SC CIC Program Coordinator Caitlin Scroggins at annual South Carolina Primary Healthcare Association Annual Conference and Board Governance Retreat.

SC CIC Director, Ryan Truskey, participating as a panelist at the National Governor's Association

Cyber Security Awareness Month

In October, SC CIC hosted several events for cybersecurity awareness month.

Your Cyber Survival Kit: An SC CIC Services Overview

An opportunity for participants to ask the SC CIC team questions and gain additional insight into the current services available to them.

Defending Against the Cyber-Scaries: Building a Security Awareness Program That's Frightfully Effective

A virtual training focused on equipping CLOs with tools and questions to assist with building an efficient security awareness program for organizations.

Battle of the Cyber Apocalypse

A virtual CTF event designed to help CLOs learn and test new cybersecurity skills. Partnering with Corelight, SC CIC had 22 participants participate in the various scenarios both in- person and virtually.

SC CIC Cybersecurity Advisor, Tim Larkin, at the SC School Board Insurance Trust (SCSBIT)'s annual "Risky Business" Conference

2025 EDTECH

Also in October, SC CIC partnered with the South Carolina Department of Education (SCDE) to present at the 2025 EDTECH Conference in Myrtle Beach, SC. SC CIC and SCDE facilitated a cyber tabletop exercise (TTX) focusing on a ransomware incident. This opportunity gave SC school district technology stakeholders to discuss critical questions that should be taken into consideration when responding to similar incidents. SC CIC hopes to carry these discussions forward in 2026 to help equip critical infrastructure organizations with the tools and questions necessary to proactively secure their infrastructure.

2025 SC CIC Conference

In August, SC CIC hosted its second cybersecurity conference in Columbia, SC, attended by more than 120 CLOs.

The SC CIC Conference gave participants the opportunity to network and exchange ideas with fellow CLOs and other cybersecurity experts.

Key Speakers

- **Pamela Evette** | SC Lieutenant Governor
- **Chief Mark Keel** | SLED
- **Gerry Auger** | Simply Cyber
- **Kevin Sherry** | DarkWebIQ
- **Cristian Rodriguez** | CrowdStrike
- **Mike Holcomb** | Fluor
- **Stef Rand** | Red Canary

Key Topics

- Industrial Control Systems (ICS) security
- Supply chain attacks
- Cyber incident response and insurance
- Threat landscape trends

SC CIC Program Coordinator Katie Scroggins, Paul Ihme, Tom Zych, & Lyde Graham during the Cyber Insurance Panel.

SC CIC Director Ryan Truskey, and SC Lieutenant Governor Pamela Evette

FoxPick: Lock Pick Village

FoxPick hosted a hands on physical security and interactive training experience allowing conference attendees to explore vulnerabilities in locks and practice their lockpicking skills in a supervised environment.

SC CIC received wholly positive feedback from the attendees and plans to host another conference in 2026.

Significant Cyber Incidents

In 2025, SC CIC responded to 85 significant cyber incidents impacting critical infrastructure in South Carolina. The sector that experienced the highest number of incidents in 2025 was the Government Facilities Sector with 66 incidents. This was followed by the Emergency Services with nine incidents. It should be noted that this disparity can be partially attributed to the distribution of sector participation in SC CIC, as government facilities continue to be the highest represented sector, accounting for 57% of SC CIC organizations.

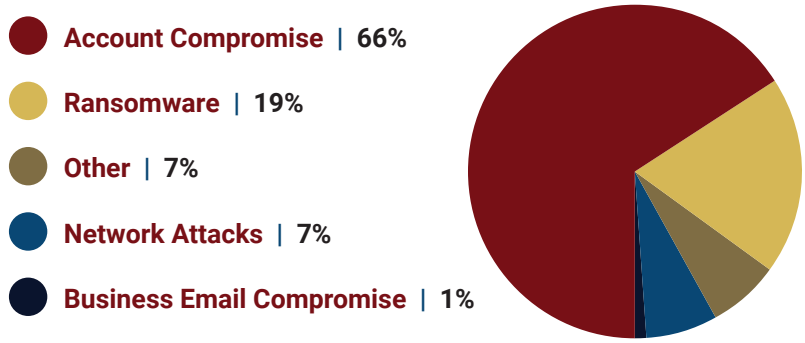
85
Significant Incidents

78%
Incidents occurred in the Government Facilities sector

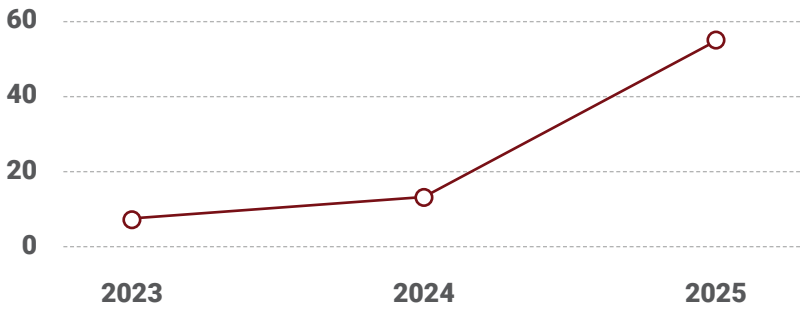
The most common type of incident in 2025 was **account compromise.**

This continuing trend was first identified and defined in the 2024 SC CIC End of Year Report. Account compromise occurs when attackers gain unauthorized access to a legitimate account, enabling further malicious actions. This can happen, for example, if a user enters their credentials on a fake login page after clicking a phishing link. Several of the SC CIC services can assist with mitigating the risks of account compromise. Those include the AD Security Assessment, Microsoft 365 Security Assessments, threat intelligence, and phishing & security awareness services. The persistence of this trend reinforces SC CIC's decision to continue allocating resources to prevent account compromise.

2025 South Carolina Incident Types



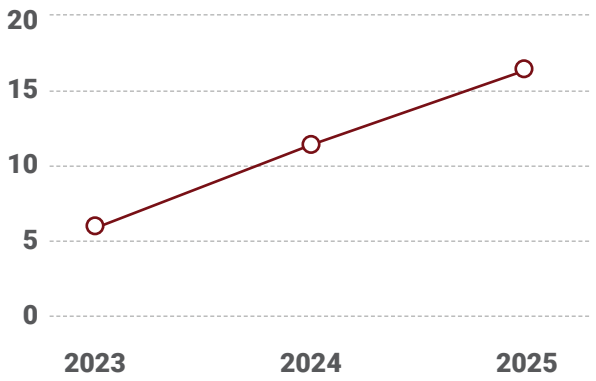
Account Compromise Trends



The second most common incident encountered this year was ransomware, a type of malware that encrypts data to block system access and disrupts the availability of network resources.

Due to ransomware's prevalence and potentially devastating effects, SC CIC tracks it separately from other malware. As suggested by its name, threat actors typically demand a ransom from the victim to restore assets. A method known as **double extortion ransomware** has also remained popular. This adds an additional step of copying and exfiltrating data prior to encryption and then demanding payment for the recovery and/or prevention of release of the data.

Ransomware Trends from 2023 to 2025

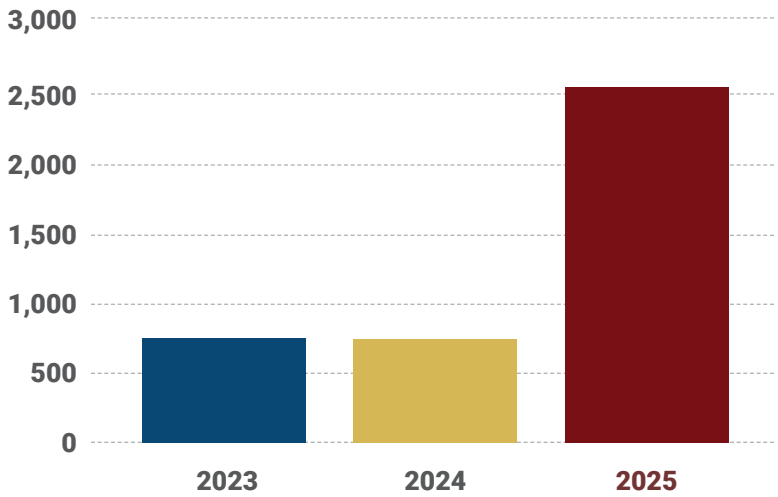


SC CIC takes a proactive approach to identifying and notifying ransomware victims. This is accomplished through monitoring deep and dark web posts for proof of network access, samples of stolen data, or other indicators of unauthorized access within an environment. Once a potential victim based in South Carolina is identified, SC CIC will contact the organization to verify the suspicious activity, and provide assistance and resources as requested by the victim. Due to the proactive approach that SC CIC takes with incidents, the team has found continuing success in making notification prior to encryption and data exfiltration, minimizing the impact of the event.

Incident Response

SC CIC's Incident Response (IR) efforts include assisting both SC CIC members and non-participants that fall under critical infrastructure in South Carolina by providing malware analysis, event log analysis, incident coordination, secure out-of-band communications, and cybersecurity consultation. This year, SC CIC analyzed more than 2500 files and websites for potential malware or other malicious intent, which represents a major increase from the previous year.

Analyses Performed by Year



2025 Incident Highlights

School District Ransomware Incident

June 2025

In June, SC CIC responded to a ransomware incident involving a South Carolina school district. The incident resulted in significant operational disruption, including payroll processing, SAT/ACT testing, and the start of summer school.

The investigation determined that initial access occurred in **April 2025** when a teacher visited a compromised website. The website delivered a malicious "**ClickFix**" payload after the user completed a fake verification process. Following execution, the payload installed a **remote access trojan (RAT)** on the employee's device.

During post-exploitation activity in June 2025, the actor performed both host and domain enumeration, then tampered with or removed security controls, including the endpoint detection and response (EDR) agent.

Insecure active directory (AD) configurations allowed the threat actor to **escalate privileges** and **obtain domain administrator access**. This enabled lateral movement to the domain controller, where the actor staged two scripts and used **PsExec** to deploy the ransomware encryptor across the organization's environment.

Utilities Ransomware Incident

June 2025

A second ransomware incident impacting a utility company occurred in June 2025. Initial access was achieved when an IT employee used a domain administrator account to install a malicious package, containing both a legitimate PuTTY application and a remote access trojan (RAT), found on a typosquatted domain impersonating the legitimate PuTTY website.

Following initial compromise, the **threat actor** deployed additional **command and control (C2)** tooling on the impacted system. The beacons utilized by the threat actor were **renamed to resemble legitimate software.** They then **abused a legitimate cloud service** present on the system to facilitate lateral movement to other devices within the environment. Additional **C2 beacons were deployed to maintain persistence**.

Due to the threat actor having domain administrator privileges, the **domain controller** was accessible without additional privilege escalation. They were also able to access the **operational technology (OT) network**, impacting systems responsible for **Industrial Control Systems (ICS)** operations.

The threat actor conducted **data exfiltration** from the **file server** using an open-source backup tool. Once complete, **PSExec and two batch scripts** were utilized to deploy the **ransomware encryptor** across all devices within the domain.

Hospital Ransomware Incident

July 2025

In July 2025, SC CIC responded to a ransomware attack impacting a regional hospital. This incident resulted in a complete halt in medical operations and a full diversion of all patients to other nearby healthcare facilities.

Investigation determined that the threat actor gained initial access to the organization's virtual private network (VPN) by brute-forcing a weak password. The compromise occurred because the organization's VPN did not enforce multi-factor authentication (MFA).

After establishing access, the threat actor conducted internal network and domain enumeration and achieved lateral movement using remote desktop protocol (RDP). The actor then established multiple internal footholds, performed credential dumping, and progressively escalated privileges until obtaining domain administrator access and control of the domain controller.

The threat actor conducted data exfiltration by transferring terabytes of sensitive data to Wasabi cloud storage. Following exfiltration, the actor staged an encryption tool in the domain controller and deployed a Group Policy Object (GPO) across the network, thus initiating organization wide encryption.

Organizations that do not require multi-factor authentication (MFA) for VPN access are significantly more vulnerable to compromise. During 2025, SC CIC responded to at least four ransomware incidents that originated from VPN services lacking MFA protections.

SLED Computer Crimes, in coordination with SC CIC, obtained a warrant for the Wasabi storage account, successfully retrieved the exfiltrated data, and returned it to the hospital. This incident represents a rare case in which the organization was able to recover all stolen data before it was released on the dark web.

Services Provided

229
Organizations using threat intelligence services

1057
Leaked credentials were identified

Threat Intelligence

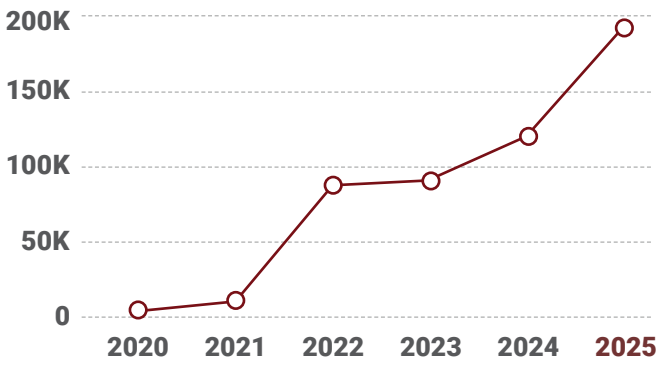
By the end of 2025, approximately 229 organizations were using SC CIC threat intelligence services, representing over 11% growth from the previous year.

Monitoring of the collective state attack surface is conducted through integrated intelligence platforms and enhanced by SC CIC's unique access to restricted, non-public sources, including dark web marketplaces, where illicit actors trade compromised data and tools, as well as restricted forums in which threat actors exchange techniques and information. This access enables the timely identification of high-value threat intelligence, such as the illicit sale of compromised network access, which is not available through public channels.

A core strength of the SC CIC threat intelligence program is through the delivery of actionable and relevant intelligence via tailored bulletins. These can range from technical alerts for IT staff to general awareness bulletins for the broader workforce.

SC CIC continuously monitors a variety of intelligence sources that host, distribute, or sell stolen credentials in order to alert participants when organization login information is exposed. These sources typically include breach-related website leaks and malware logs collected from threat actor controlled servers operating infostealer malware. This compromised data is frequently aggregated and sold on dark web marketplaces, making it accessible to a broad range of cyber threat actors. Stolen credentials are a common method for achieving initial access to an organization's internal network and often precedes more severe attack phases, such as ransomware deployment. In 2025, SC CIC identified and shared **1057 leaked credentials** obtained through the indexing of malware logs, primarily associated with **infostealers** such as **RedLine, Rhadamanthys, and Vidar.**

Total Monitored IP Addresses

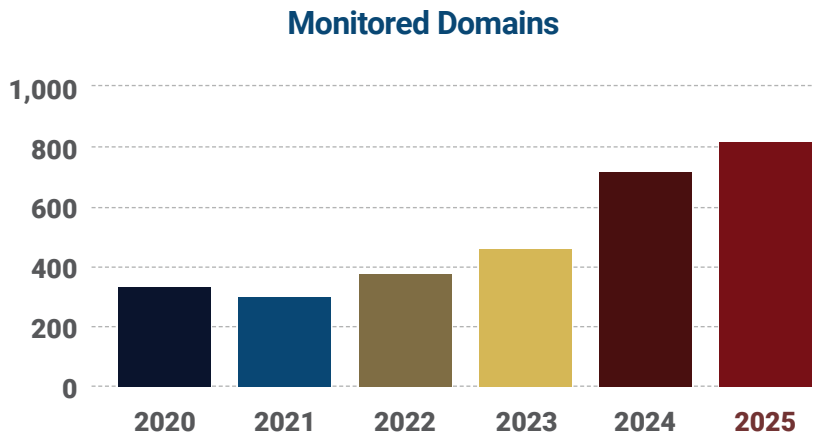


By the end of 2025, SC CIC was also continuously monitoring **930 unique IP ranges** belonging to participating organizations, **encompassing 193,923 IP addresses**. This capability enabled SC CIC to issue **55 notifications** during the year related to risky or exposed services.

These alerts included exposures to zero-day vulnerabilities as well as insecure services such as Telnet, Server Message Block (SMB), and Remote Desktop Protocol (RDP) that were enabled and publicly accessible.

In addition, SC CIC actively monitors **807 domains** associated with participants for unintended public exposure, dark web presence, and potential compromise. This monitoring resulted in **495 deep and dark web alerts**. Some of these alerts leverage **optical character recognition (OCR)** technology to detect participant names or logos appearing on suspicious websites, such as fraudulent landing pages designed to harvest user credentials.

More than 10% of these alerts involved participant data exposed through **breaches of third-party organizations or vendors**. These alerts not only help participants understand their exposure but also ensure awareness of third-party incidents that may not have been formally disclosed. In connection with third-party breaches, SC CIC collected **683 leaked credentials** on the dark web via third-party breaches during 2025.



Threat Intelligence Successes

- A successful threat intelligence bulletin from this year included alerts regarding the abuse of **Microsoft Direct Send** during the **Summer of 2025**. SC CIC's early notification allowed participants to review and adjust their configurations ahead of widespread exploitation across the state.
- End user threat bulletins were particularly well received within the CLO network, with many CLOs expressing appreciation for the concise format that effectively educated staff on emerging cybersecurity threats. Consistent participant feedback highlights SC CIC as a primary, and often initial, source of notification for actionable security threats.
- Another notable success involved a newly discovered **Cisco Adaptive Security Appliance (ASA) SSL VPN zero-day vulnerability** that was actively being exploited. Using our attack surface monitoring platform, we promptly alerted all participating organizations whose **Cisco Adaptive Security Appliance (ASA) SSL VPN web portal** was exposed to the internet and potentially vulnerable to exploitation.
- In one significant incident involving a third-party emergency management platform, attackers posted more than 80,000 leaked credentials on a ransomware extortion site. After indexing this data, **SC CIC was able to notify 103 unique participating organizations and provide each with a targeted list of affected users.**

Readiness Exercises

This year SC CIC continued to build upon the success of our readiness exercise service established in 2024. These readiness exercises offer an immersive way for organizations to evaluate and enhance their ability to detect, respond, and recover from cyber threats.

While modeled after traditional tabletop exercises, these engagements provide more customization options and the ability to integrate technical injects that simulate real attacker behavior. Participants work through realistic scenarios that test both procedural workflows and technical capabilities, helping teams validate response plans, uncover operational gaps, and strengthen the full incident response lifecycle.

By combining **structured decisionmaking with hands-on emulations**, such as simulated malware persistence, these exercises deliver a comprehensive view of organizational readiness. It also fosters cross-department collaboration, improving coordination and accelerating effective response. Each engagement can be tailored to accommodate the unique maturity level of the organization, offering foundational insights for emerging teams and advanced threat simulations for seasoned defenders.

Once the exercise is finished, organizations receive an exhaustive **after action report** that provides an Executive Summary designed for leadership. These summaries highlight critical objectives, findings, and strategic recommendations. Each gap is paired with practical, targeted steps to improve the skills and capabilities evaluated during the exercise.

The report also conducts a comprehensive analysis of the organization's performance, featuring:

- An overall maturity rating
- Phase-by-phase incident response maturity scores
- Clearly identified weaknesses

Throughout 2025, SC CIC completed readiness exercise engagements with 14 organizations, including four that incorporated adversary emulation for a more advanced assessment.

Looking ahead to 2026, enhancing adversary emulation campaigns will remain a priority as we continue supporting organizations in building stronger, more resilient security programs.

> *Our experience utilizing the SC CIC readiness exercise was highly valuable in assessing our preparedness and response capabilities. The exercise provided actionable insights, helped identify key areas for improvement, and strengthened our coordination across teams.*
>
> **School District of Pickens County**

> *The readiness exercises we've done with SC CIC have been very valuable. The first one we did in 2024 allowed us to examine our newly created Incident Response Plan, with senior management. It revealed a need for creating some one-page response flowcharts. In 2025, we discovered some holes in our security and because it was "budget season", we were able to get the needed items in the budget. Thanks SC CIC!*
>
> **Broad River Electric Cooperative**

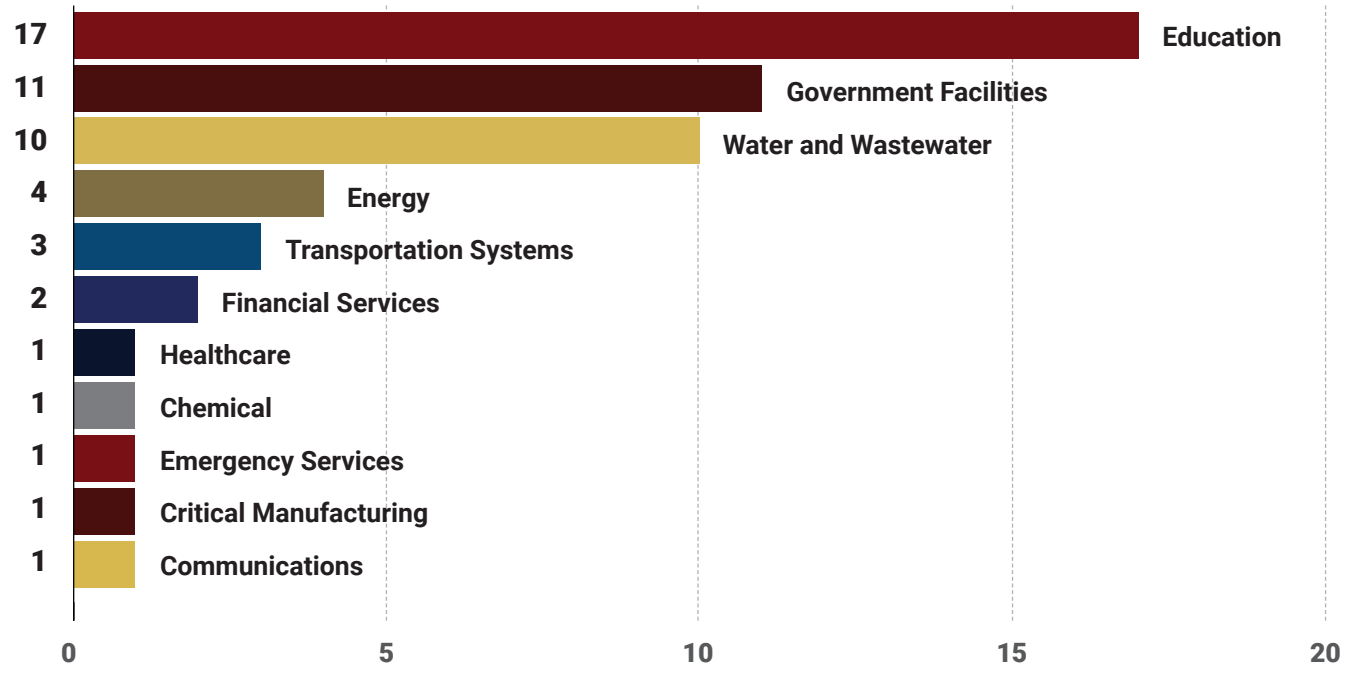
Active Directory Security Assessment

Active Directory (AD) serves as the core identity and access management system for most enterprise networks worldwide.

Its widespread use and the vital functions it supports makes it an attractive target for attackers attempting to disrupt organizational environments. To help safeguard this critical component of participants' infrastructure, SC CIC created the **AD Security Assessment** service. This service is designed to give organizations a clearer picture of their AD security health and provide practical steps to lessen the chances and consequences of a security breach.

In conducting an AD assessment, SC CIC leverages a set of tools to analyze the participant's AD environment and uncover weaknesses, configuration issues, and potential attack routes that adversaries might exploit. After the review, participants receive a comprehensive report summarizing the issues identified, recommended fixes, and additional resources to help them better understand their AD landscape. SC CIC analysts are also available to offer follow-up guidance and support to CLOs as needed. The assessment produces a risk score that helps quantify security improvements over time; **fewer issues result in a lower—and therefore stronger—score**. These measurements also allow SC CIC to observe security patterns across various sectors and across the state, improving its ability to assist all participants effectively.

Number of AD Security Assessments by Sector



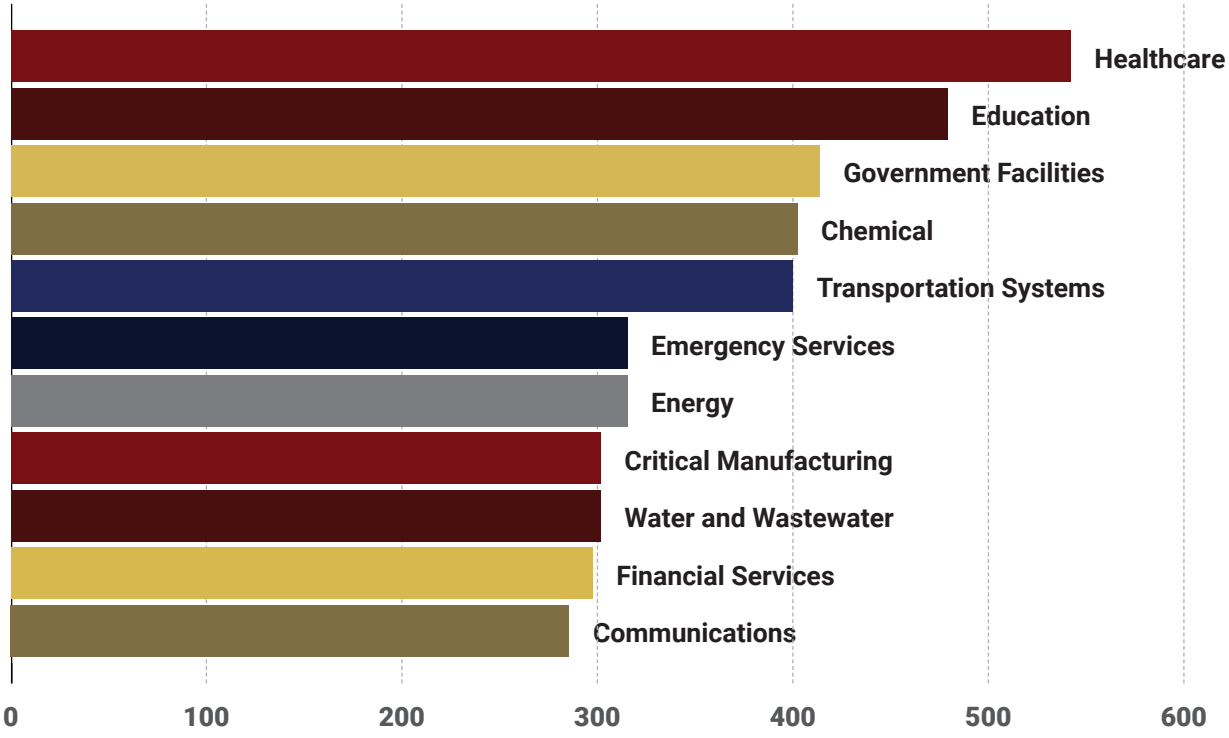
As shown in the chart below, the healthcare subsector now has the highest average score across AD assessments conducted since 2022, indicating a greater prevalence of weaknesses, vulnerabilities, and misconfigurations compared to other sectors. This represents a shift from last year, when the education sector held the highest average score. The increased focus on the education sector this year, with 17 assessments completed, as shown in the previous chart, enabled organizations to implement critical security improvements within their environments. As a result, the sector's average score declined significantly, reflecting measurable security maturity gains. The SC CIC average as a whole for scans conducted in 2025 alone seen a **22% improvement** as compared to 2024. This improvement is largely driven by organizations conducting multiple scans throughout the year and applying targeted security changes. Among organizations with multiple scans, the average score improvement was 23%, underscoring the value of repeated assessments and proactive remediation.

52
AD assessments completed

42
Organizations assessed

22%
Improvement in scan since 2024

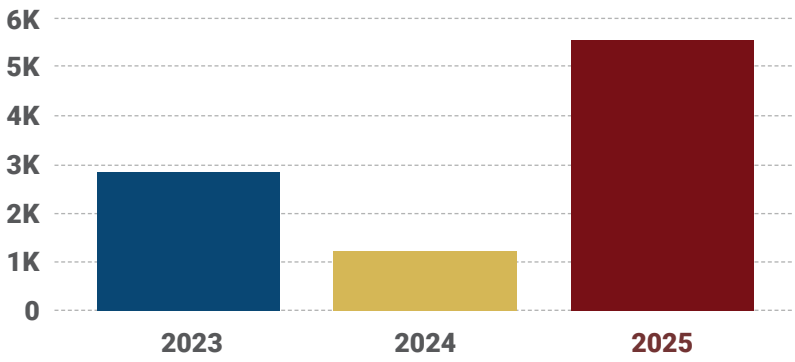
Average AD Security Assessment Score by Sector



Simulated Phishing and Cybersecurity Training

Threat actors continue to see success with their phishing campaigns, resulting in it being a commonly utilized attack method in cyber incidents. To combat the ever-present threat of phishing attacks in 2025, SC CIC has prioritized the facilitation and dissemination of **user education to partner organizations**. This led to a significant increase in the number of training units distributed to end users.

Number of Training Units Disseminated to Participant Organizations



In 2025, SC CIC provided 30 phishing campaigns to 19 different organizations.

16,842
Phishing emails sent

49.73%
Emails opened

5.37%
Links clicked

3.66%
Entering credentials

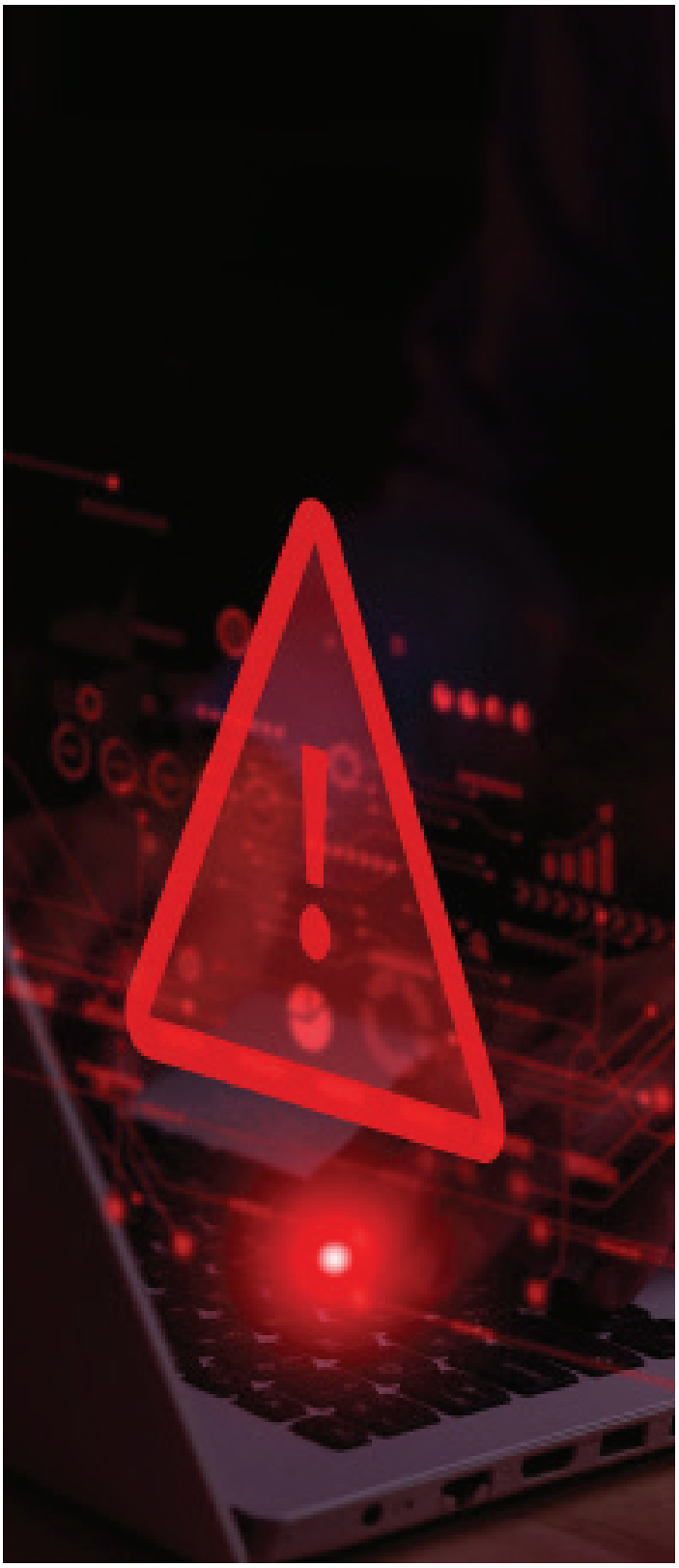
By preventing the extraction of credentials from these malicious pages, SC CIC significantly impedes the spread of attacks within South Carolina and beyond.

This training is designed to reenforce safe online practices as well as inform users of emerging threats. As new attack techniques are identified, the SC CIC team prioritizes training on that front. For example, when ClickFix/Fake Captcha attacks started to become more common, SC CIC moved quickly to provide training on the topic to 653 users.

Beyond conducting phishing simulations and providing user awareness training, SC CIC has the ability to proactively disrupt the infrastructure used to support phishing campaigns. These attacks commonly rely on fraudulent web pages designed to imitate legitimate authentication portals to capture user credentials. When a user unknowingly enters their login information, the credentials are intercepted by threat actors and subsequently used to gain unauthorized access and conduct follow-on attacks.

Upon identifying such malicious sites, SC CIC works closely with its partners to rapidly take them offline. Once disabled, any associated links contained within phishing emails become ineffective, no longer leading to credential harvesting pages. By preventing the collection of user credentials through these malicious sites, SC CIC reduces the ability of threat actors to propagate attacks within South Carolina and beyond.

Throughout 2025, **SC CIC successfully deactivated 328 malicious websites** used in such attacks and notified 70 organizations of compromised accounts within their systems. In addition to the notification, our team also provided guidance on recovering and securing the account(s). This allowed the affected organizations to swiftly respond and secure the accounts, preventing further impacts. **Given the nature and rapid spread of phishing attacks, combating them necessitates the multi-pronged approach SC CIC has developed**. This includes comprehensive user training, rapid attack identification, disrupting attacker infrastructure, quick account recovery, providing aid to organizations in recovering compromised accounts, and fortifying overall account security.



328
Malicious websites successfully deactivated

70
Organizations notified of compromised accounts

Vulnerability Scanning

One of the services SC CIC offers is external vulnerability scanning. By leveraging Nessus through Tenable cloud scanners, we can obtain an accurate perspective of a potential malicious attacker when they encounter the organization's internet facing assets. Having this perspective grants us valuable insight into an asset's common initial network access vector as well as how to remediate and secure it. Once the scan is complete, an SC CIC analyst then reviews the scan results and creates a succinct personalized report containing recommendations for remediation. These solutions are formulated based on various factors, such as expected impact and exploitation probability. Additionally, we offer verification scans on demand to ensure the vulnerabilities are remediated once the solutions from the report are implemented.

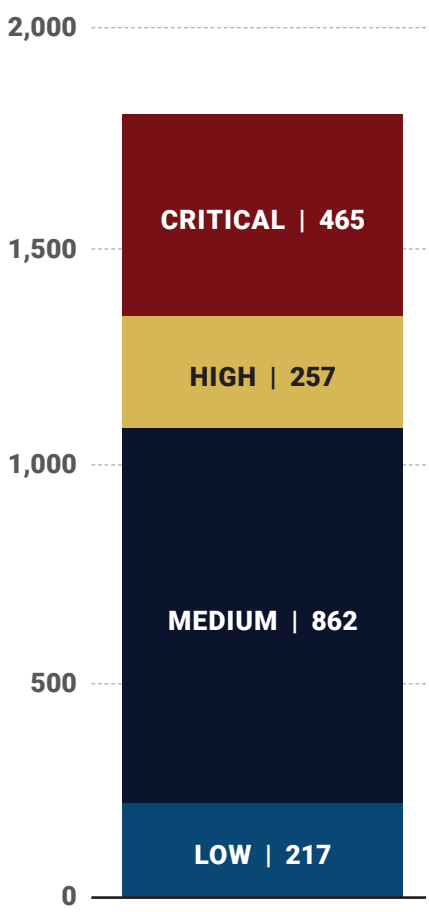
173
Organizations scanned for vulnerabilities

1,801
Vulnerabilities detected

HTTP Strict Vulnerability

One common vulnerability we encountered this year involved a lack of HTTP Strict Transport Security (HSTS) enforcement, as is defined by RFC 6797. HSTS is an optional response header, which is configured on the server to instruct the browser to communicate solely using HTTPS. If HSTS is not enforced, it leaves communication channels exposed to various attacks, including but not limited to SSL-stripping man-in-the-middle attacks and downgrade attacks; it also weakens cookie-hijacking protections that may be in place. Configuring the server to use HSTS strengthens the security posture of South Carolina's critical infrastructure data and resources used by employees and citizens all throughout the state.

Vulnerabilities Discovered by Severity



Microsoft 365 Security Assessments

Microsoft 365 (M365) is essential for modern business productivity, but its complexity and constant exposure to evolving threats make it an attractive target for cybercriminals.

Many organizations struggle to properly configure M365's security controls, manage user access, and maintain compliance, which can lead to misconfigurations, data exposure, and risks such as unauthorized access or business email compromise.

To address these concerns, **SC CIC introduced a new service this year**; our Microsoft 365 Security Assessment. This service is designed to help organizations navigate these challenges and strengthen their security posture. By utilizing Soteria's 365 Inspect tool, a comprehensive review of the M365 tenant is conducted, examining identity security, email protections, data loss prevention, auditing, and compliance settings. This visibility allows SC CIC to identify vulnerabilities and provide detailed, prioritized recommendations. Participants receive access to a dashboard to review their findings, a full report for each scan, and access to monthly webinars highlighting common issues and trends to ensure clear understanding. Our analysts remain available for follow-up support, helping organizations implement improvements and confidently secure their M365 environment.

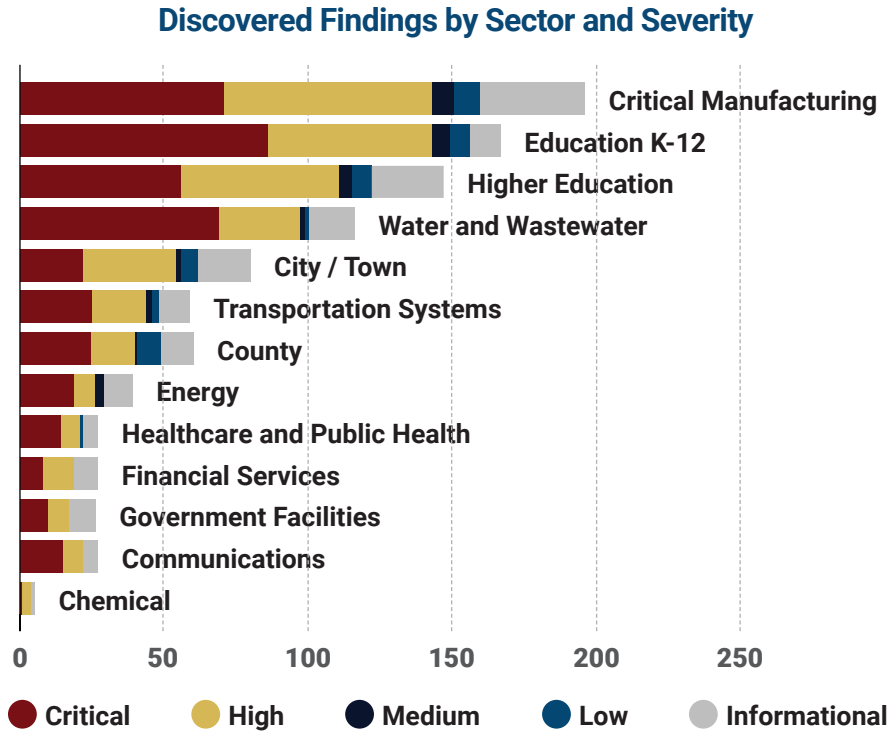
In 2025, 63 organizations began utilizing M365. This resulted in the discovery of:

436
Critical findings

325
High-severity findings

29
Medium-severity findings

43
Low-severity findings



SLCGP Services

The State & Local Cybersecurity Grant Program (SLCGP)[2] is a federal grant program overseen by the Department of Homeland Security (DHS). The mission of SLCGP is to help state, local, tribal, and territorial (SLTT)[3] governments mitigate against cybersecurity risks and threats to information systems owned or operated by—or on behalf of—SLTT governments. SC CIC spearheaded the SLCGP for South Carolina, leveraging its existing network of trust built with critical infrastructure organizations across the state to create a robust and diverse Cybersecurity Planning Committee, which then co-authored the South Carolina Statewide Cybersecurity Plan[4] in late 2023. This effort is continuous and iterative to adapt to new threats and challenges as they are identified throughout the state.

With eligible entities being able to apply for funding to improve their organization's security posture, SC CIC has secured funding for several services available to qualified organizations across South Carolina. Eligible entities should visit Grants | South Carolina Critical Infrastructure Cybersecurity for additional information and next steps.

2. https://www.cisa.gov/cybergrants/slcgp 3. https://www.cisa.gov/audiences/state-local-tribal-and-territorial-government 4. https://sccic.sc.gov/sites/sccic/files/Documents/SC%20Cyber%20Plan.pdf

Endpoint Detection & Response (EDR) and Managed Detection & Response (MDR) Solution

SLED has partnered with Check Point Software Technologies and The Teneo Group to offer advanced cybersecurity services to local South Carolina government through the US Cybersecurity and Infrastructure Security Agency's (CISA) State and Local Cybersecurity Grant Program (SLCGP).

With the Checkpoint EDR and MDR solution, eligible organizations have access to the following products:

Endpoint Detection and Response (EDR)

- **Real-Time Monitoring:** Continuously monitoring of endpoint devices to detect and prevent advanced malware, ransomware, and other threats.
- **Automated Response:** Rule-based responses to potential threats, preventing lateral proliferation across the network.
- **Comprehensive Coverage:** Protection includes anti-ransomware, anti-malware, anti-bot, anti-exploit, behavioral guard, and port protection.

Managed Detection & Response (MDR)

- **24/7/365 Monitoring:** SOC analysts continuously monitor data and alerts, prioritizing and neutralizing threats in real time.
- **AI & Human Expertise:** Combines cutting-edge AI with experienced analysts to reduce alert fatigue and identify behavior-based threats, including zero-day attacks.
- **Proactive Defense:** Continuous monitoring and proactive threat hunting to detect and respond to attacks swiftly.

Incident Response Services

- **Immediate Action:** Containment and remediation of cyberattacks with real-time data access and forensics analysis.
- **Expert Guidance:** Detailed documentation and best practices to enhance processes, response speed, and compliance.
- **Custom Security Enhancements:** Tailored recommendations and protections to fortify your cybersecurity posture and prevent future attacks

Since the implementation of this service in 2024, 14 participants have engaged in the service, enabling 22,484 endpoints to be protected by Check Point's Endpoint Detection and Response (EDR) solution.

14
Participants since 2024

22,484
Endpoints protected by Check Point's EDR solution

CyberDefenders

CyberDefenders is an online cybersecurity training platform that hosts many different labs covering relevant cybersecurity topics and skills. The goal of providing CyberDefenders to eligible organizations is to give information technology (IT) and information security (INFOSEC) professionals hands-on experience and training that is invaluable in the unending process of securing an organization's infrastructure. The available labs include malware analysis, threat intelligence, network forensics, detection engineering, threat hunting, and cloud and endpoint forensics. At the completion of 2025, the first year of this service, there are **82 participants** engaged in CyberDefenders training.

82

Participants comprised the first year of CyberDefenders training

CyberBit Cyber Range Exercises

Launched in November of 2025, CyberBit cyber range exercises is the newest of services available to SLCGP-eligible participants. CyberBit is a cloud-hosted platform that trains users to be cyber ready. This is accomplished through immersive and realistic exercises in a cyber range environment that mirror real-world threats.

Through the CyberBit exercises, participants will:

Build Advanced Skills

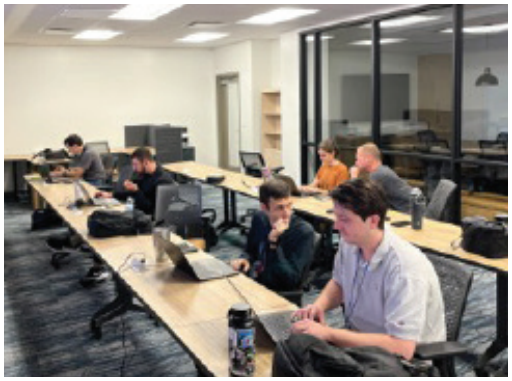
- Receive expert-led training in incident triage, digital forensics, log and network analysis, and other core disciplines.
- Increase your team's capabilities for real-world cyber incidents and boost confidence in handling complex challenges.

Validate & Strengthen Your Team

- Identify true strengths and improvement opportunities through realistic, hands-on assessments.
- Leaders receive clear guidance on training priorities and high-impact investments through exercises that delve into essential log sources, tools, and security controls.

Foster Teamwork & Camaraderie

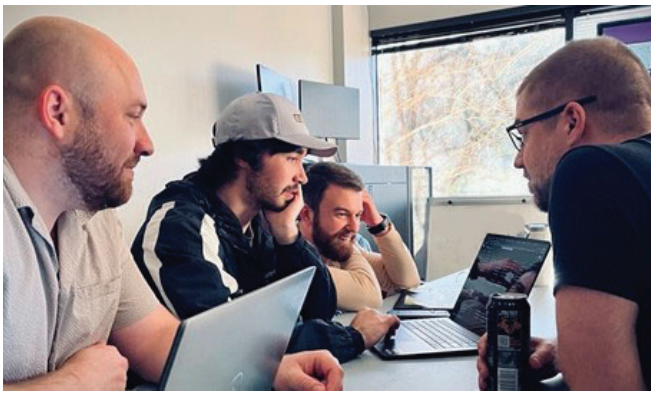
- Deepen collaboration and trust across your security team.
- Build a cohesive and resilient team through high-pressure real-life scenarios, which cultivates seamless coordination and communication.



The SC CIC team participating in a CyberBit cyber range exercise at SLED headquarters

Conclusion

SC CIC remains committed to improving the cybersecurity posture of each critical infrastructure organization in South Carolina. Our team is continuously evolving through the pursuit and cultivation of partnerships as well as the implementation of innovative solutions, as is exemplified in our new service offering: the Microsoft 365 (M365) Security Assessments, establishing opportunities for external partners to engage in SC CIC, and to secure funding to expand the SC CIC team.



SC CIC plays an integral role in equipping South Carolina's critical infrastructure to defend against emerging and existing cyber threats, but that can only be achieved by our members' dedication. Every stakeholder involved plays a critical role in the continuance of our mission by supporting SC CIC's unique culture.

Looking Ahead

As SC CIC moves into 2026, there are several key initiatives that SC CIC is looking to implement.

- **The first is to coordinate more in-person events for both technical training and networking for information security professionals and cybersecurity students across South Carolina.**
- **The second is to continue advancing the SC CIC team forward with the hiring of new positions, along with proactively training on relevant topics.**
- **The final initiative is to continue pursuing growth in both participating organizations and partnerships in both a statewide and national capacity.**

Glossary

Account Compromise: Account compromise occurs when a threat actor gains access to an account, a user's credentials or finds another way to act on their behalf.

Active Directory (AD): A Microsoft directory service for the management of identities in Windows domain networks.

Adversary-in-the-Middle: A type of cyberattack where an attacker intercepts or manipulates communications between two parties without their knowledge, often to steal or alter information.

Azure: Microsoft's public cloud computing platform.

Brute Force: In cryptography, a brute-force attack is a method of obtaining legitimate credentials by systematically trying all possible combinations of passwords, encryption keys, or other secrets until the correct one is found.

Capture the Flag (CTF): A type of cybersecurity competition where individuals or teams are challenged to demonstrate their computer security skills, often by discovering strings of text that represent a "flag".

Cybersecurity and Infrastructure Security Agency (CISA): The US operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

Cisco Adaptive Security Appliance (ASA): Cisco security devices created to protect corporate networks.

ClickFix: A tactic utilized by threat actors where users are presented with seemingly helpful solutions- such as prompts that instruct users to open a terminal or the Windows Run Dialog box and execute an arbitrary command.

Command and Control (C2): Is a set of tools and techniques that threat actors use to maintain communication with the compromised device or endpoint.

Conditional Access: A security feature that ensures the individual seeking access to a system is the authorized party. This consists of an evaluation of certain criteria before access is granted such as the user's location, device compliance, or presence on a trusted network.

Credential Harvesting: A cyberattack where attackers collect usernames, passwords, or other sensitive information, typically through phishing, malware, or fake login pages. The goal is to steal login details for unauthorized access or other malicious activities.

Critical Infrastructure: Resources whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Dark Web: A portion of the internet made up of unindexed web content requiring special software to access.

Deep Web: A portion of the internet made up of unindexed web content that is behind a paywall or protected by a password.

Defense Evasion: A tactic used by cybercriminals to avoid detection by security systems during an attack, often involving techniques like hiding malware, using encryption, or exploiting weaknesses in monitoring systems.

Domain: A network of computers and devices that are grouped together under a common name, often managed by a central server.

Domain Controller: A server that manages network access, authentication, and security policies within a domain.

Downgrade Attack: An attack where threat actors force the target system to switch to a low-quality, less secure protocol or encryption standard.

Encryption: The process of converting plaintext data into a coded format to prevent unauthorized access. Only those with the correct decryption key can read the original data.

End users: Someone who accesses computer systems and applications for the purpose of doing their job. End users typically do not have in-depth knowledge of the technical details of the systems they use.

Endpoint Detection and Response (EDR): A cybersecurity solution designed to monitor, detect, and respond to suspicious activity on endpoints (such as computers and servers), helping to identify potential threats before they can cause significant damage.

Event Log: A record of events or activities on a computer system or network, often used for troubleshooting, monitoring, and security analysis. Event logs track user actions, system errors, or abnormal behavior.

Executable: A type of computer file that can be run or executed on a computer, typically containing instructions for the computer to perform a task. Executables can be applications, scripts, or malware.

Exfiltration: The unauthorized transfer of data from a system or network to an external location. This can be done by attackers to steal sensitive information like personal data, intellectual property, or login credentials.

Industrial Control Systems (ICS): Systems used to monitor and control industrial processes such as manufacturing, power generation, and water treatment. These systems are critical for the operation of essential infrastructure and can be vulnerable to cyberattacks.

Indicators of Compromise (IoC): A technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.

Infostealer: "Information stealer"; malware that is designed to steal victim data such as usernames or passwords that can be sold or used to further compromise a network.

Initial Access: The first phase of a cyberattack where an attacker gains access to a system or network. This may involve exploiting vulnerabilities, phishing, or using stolen credentials.

Kerberos Ticket Granting Ticket (KRBTGT): A special ticket used by the Kerberos authentication protocol to authenticate users and services in a network. The KRBTGT is used to obtain service tickets for access to resources. The Kerberos protocol facilitates secure, passwordless proof of identity over a non-secure network. It is a key component of many network security solutions.

Malware: Any software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Managed Detection & Response (MDR): A cybersecurity service that proactively protects organizations from cyberthreats using advanced detection and rapid incident response.

Managed Security Service Provider (MSSP): A third-party organization that provides outsourced monitoring and management of security services for businesses, including threat detection, vulnerability management, and incident response.

Microsoft 365 (M365): A cloud-powered subscription service that provides productivity and collaboration apps, along with cloud services.

Microsoft Direct Send: A method used to send emails directly to an Exchange Online customer's hosted mailboxes from on-premises devices, applications, third-party cloud services using the customer's own accepted domain.

Microsoft Exchange: A collection of applications that enable digital messaging and collaboration in an enterprise IT environment that typically consists of Microsoft Exchange Server and Microsoft Outlook.

Multi-Factor Authentication (MFA): Authentication method that requires the user to provide two or more verification factors to gain access to a resource.

Nessus: A security tool used to scan assets and identify known vulnerabilities that could be exploited.

NodeSnake: A JavaScript-based malware that requires Node.js to execute.

OpenAI: An Artificial Intelligence (AI) research and deployment company that produces services such as ChatGPT.

Operational Technology (OT): Programmable systems or devices that interact with the physical environment. These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events.

Optical Character Recognition (OCR): A technology that identifies and extracts text from unstructured documents like images, screenshots, and physical paper documents.

Out-of-Band: Information transmitted through a communications channel separate from the primary.

Persistence: In cybersecurity, this occurs when a threat actor discreetly maintains long-term access to systems despite disruptions to connections such as restarts or changed credentials.

Personally Identifiable Information (PII): Anything that can be used to identify an individual (e.g. Social Security Number (SSN), driver's license number, address, phone number, financial account number).

Phishing: The practice of sending fraudulent communications that appear to come from a legitimate source with the goal of stealing money, gaining access to sensitive data and login information, or to install malware on the
victim's device.

Privilege Escalation: The process by which an attacker gains elevated access to resources or permissions that are normally restricted, typically through exploiting vulnerabilities.

PSExec: A command line tool that allows users to run programs on remote systems.

PuTTY: An open-source terminal emulator for secure remote access via SSH, Telnet, and serial connections.

Ransomware: Malware that uses encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to reinstate access.

Redline Infostealer: A malware strain designed to steal sensitive information from compromised accounts or systems. It is typically delivered via phishing emails, malicious URL links, or social engineering. It is often sold as Malware-as-a- Service (MaaS).

Remote Access Tool: A software application that allows a user to remotely control or access another computer or network. These tools can be legitimate for remote administration but are often used maliciously by attackers.

Remote Access Trojan (RAT): A form of malware that provides threat actors with remote access and control of the compromised endpoint.

Remote Desktop Protocol (RDP): Proprietary Microsoft protocol which provides a graphical interface that allows a user to connect to one computer from another computer over a network connection. While it has legitimate uses, it is commonly leveraged by threat actors to gain remote access as well.

Restic: A modern backup program for Linux, macOS, and Windows.

Reverse Proxy: A server that redirects legitimate requests from clients that can be abused to intercept user credentials, MFA tokens, and other sensitive information.

Rhadamanthys Infostealer: First discovered in 2022, Rhadamanthys is a malware strain designed to steal sensitive information or credentials via email, web injects, and malvertising campaigns. It is often sold as Malware-as-a- Service (MaaS) and is utilized by multiple threat actors.

Server Message Block (SMB): Communication protocol that facilitates connectivity within a network for tasks such as printing, file sharing, and network browsing. Microsoft systems heavily rely on this protocol, and it is a frequent vector for cyber-attacks.

Service Level Agreement (SLA): A formal agreement between a service provider and a client that outlines the expected level of service, including response times, availability, and performance metrics.

Session Token: A piece of data used to authenticate and maintain a user's session on a website or application. It is typically issued after successful login and is used to identify the user in subsequent interactions.

Stale Account: An account that is no longer in active use but has not been deactivated or removed from a system. Stale accounts can pose a security risk, as they may be exploited by attackers.

Tabletop Exercise (TTX): A discussion-based exercise where participants meet in a classroom setting or in breakout groups to validate the content of a plan by discussing their roles during an emergency and their responses to a particular situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on
the scenario.

Tactics, Techniques, and Procedures (TTPs): A term used in cybersecurity to refer to the behavior of a threat actor. These include the overall goals and strategies of an attack, the categorical methods employed, and the specific steps and tools used to engage.

Telnet: Network protocol that allows a user to log onto another computer within the same network from the command line. Telnet is considered insecure as it sends login information without encryption and can be easily intercepted during transmission.

Tenable: An exposure management company most known for vulnerability scanning and management.

Trojan or Trojan Horse: A type of malware that disguises itself as legitimate software or files and tricks users into installing it, allowing threat actors unauthorized access to their device.

Vidar Infostealer: A type of malware typically delivered via email or as ISO files that have been embedded in fake installers for legitimate software.

Virtual Private Network (VPN): A technology that creates a secure, encrypted connection over the internet, allowing users to access the web privately and safely, as if on a private network.

2025
Year In Review