

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

2023
YEAR IN REVIEW



Table of Contents

Overview 3

 SC CIC Personnel 3

 SC CIC Overall Growth 4

 Cyber Liaison Officer Program..... 5

 CLO Webinars..... 5

 External Engagements 6

 The Citadel Research Project..... 8

 SC CIC and Significant Cyber Incidents..... 9

 Incident Response 9

 Services Provided..... 13

 Cyber Posture Review..... 13

 Threat Intelligence..... 14

 Adversary Emulation..... 15

 Readiness Exercises..... 16

 Active Directory Security Assessment..... 16

 Simulated Phishing and Cybersecurity Training..... 18

 Vulnerability Scanning 19

Conclusion..... 20

Glossary..... 21

Overview

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

SC CIC services include cyber posture reviews (CPRs), threat intelligence, adversary emulation, readiness exercises, Active Directory assessments, phishing and security awareness training, and vulnerability scanning. These services have been thoughtfully chosen with the aim of making the biggest possible impact on the cybersecurity posture of the state. This is one of the many factors that make SC CIC unique. Instead of only responding to significant cyber incidents, SC CIC aims to prevent significant cyber incidents from occurring. This document will provide an overview and statistical highlights of SC CIC's efforts to protect the state's critical infrastructure in 2023.

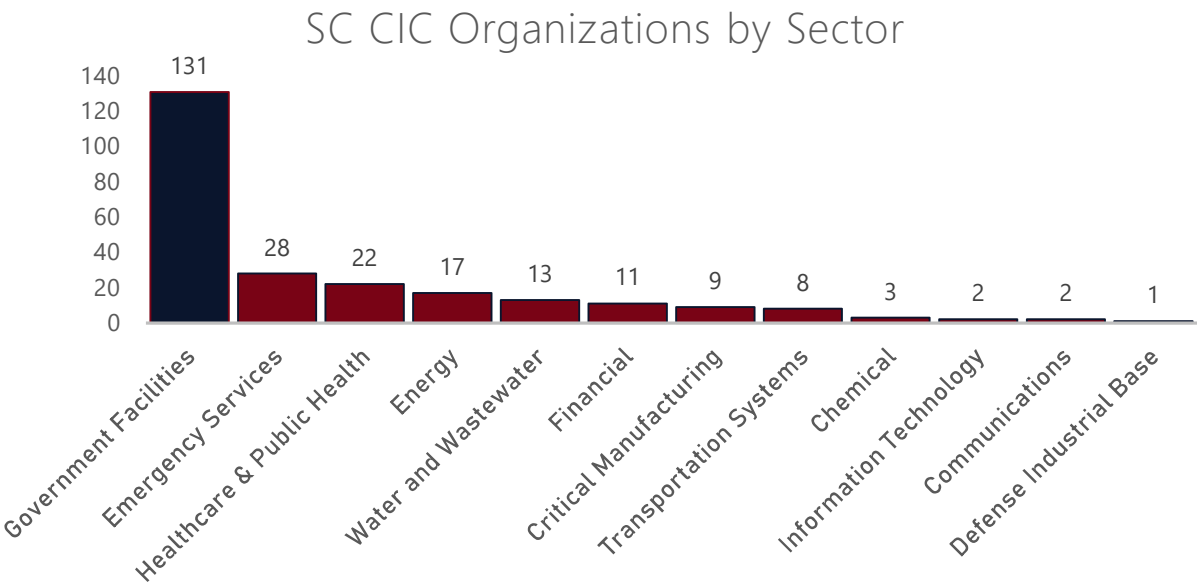
SC CIC Personnel

The strength of any great program is its people, and SC CIC is no different. The team includes the program director, four analysts with complementing security specialties, a cybersecurity advisor, and a program coordinator. With just these seven personnel, SC CIC has been able to consistently deliver exceptional results.

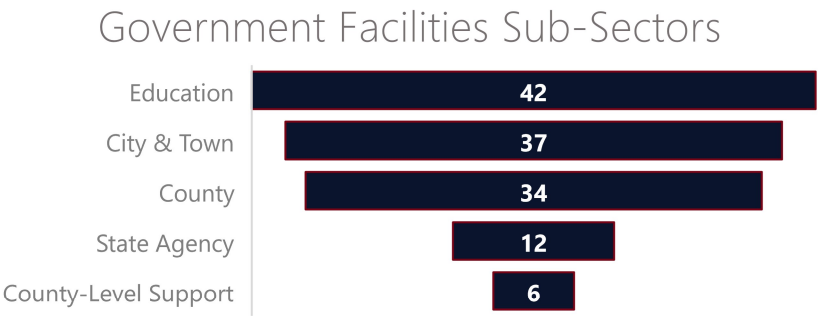


SC CIC Overall Growth

In 2023, the total number of SC CIC organizations rose to **247**, an increase of **17** from the previous year. These organizations represent **12 of the 16 critical infrastructure sectors** identified by Presidential Policy Directive 21 (PPD-21)¹. As in previous years, the largest representation is the Government Facilities sector. Since SC CIC was created to serve critical infrastructure entities operating below the State level, this sector will always be an intentional focus. The steady growth of new organizations in 2023 reflects the success of relationships built between SC CIC and new partners across all critical infrastructure sectors of South Carolina.



The Government Facilities sector is comprised of local and state government, plus education and elections. The following graph breaks down Government Facilities participation within SC CIC. The **Education** subsector is the largest participant, which includes public K-12 schools and both private and public higher education institutions. The **County-Level Support** sub-sector represents agencies that operate at the county level, such as Solicitor’s offices.



¹ https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

Cyber Liaison Officer Program

Cyber Liaison Officers, better known as CLOs, are a critical component of SC CIC. These IT professionals and administrators are responsible for coordinating their organization’s onboarding into the SC CIC program, and designating which SC CIC services they would like to utilize. **CLOs serve as the primary point of contact with SC CIC**, which fosters continuous two-way information sharing to include reporting cyber threats, incidents, or concerns that the organization faces as well as receiving and distributing threat intelligence to the people who can act on it. At the end of 2023, **the total number of CLOs participating in SC CIC was 410**, an **increase of 61** from the previous year.



CLO Webinars

SC CIC holds **monthly CLO webinars** to engage with the CLO network, deliver the latest cyber threat intelligence, maintain awareness of the current threat landscape, and to provide updates on SC CIC’s services. Occasionally, partners and CLOs are invited to share unique security perspectives and experiences with the rest of SC CIC, along with potential services that are available to participants. This year, **Soteria** presented on Business Email Compromise (BEC) and **DarkWeb IQ** provided details about a new addition to SC CIC’s offerings that they would be facilitating. Additionally, SC CIC invited esteemed representatives to participate in a **CLO panel** which discussed challenges the panelists faced within their respective sectors while working to secure their organization. SC CIC maintains focus on providing CLOs with timely, relevant, and actionable information in these monthly calls, which has fostered consistent attendance and ongoing positive feedback from attendees.

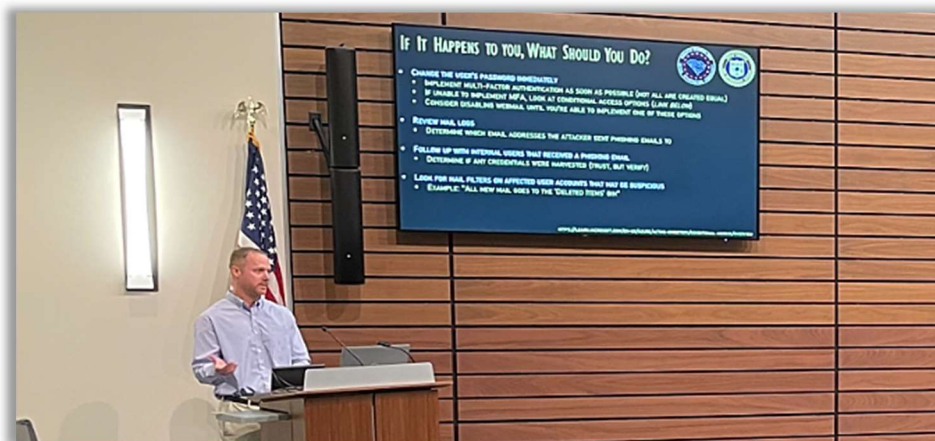
External Engagements

External engagements allow SC CIC to connect with critical infrastructure entities across the state, and then share unique insights on the state of SC cybersecurity back out to the security community. In 2023, SC CIC personnel were invited to participate in **26 events** including:

- Presenting at the **South Carolina Association of Registration and Election Officials (SCARE)** annual conference
- Presenting at the **Cybersecurity Education for Critical Infrastructure Protection Workshop**, hosted by The Citadel
- Presenting at the **SC.GMIS 2023 Management, Innovation, & Security Conference**
- Presenting at the **South Carolina School Boards Insurance Trust's** annual Risky Business Seminar
- Participating on a panel discussing the cybersecurity workforce at the **2023 State of SC Cyber Security Awareness Symposium**

SC CIC also hosted several events this year. In **February**, engineers from **Palo Alto Networks** were invited to lead a technical **Cortex XDR and XSOAR workshop**. These tools are utilized by several participants in their networks and SC CIC coordinated this event to give them direct access to expertise that would help leverage them most effectively. CLOs were first given tutorials and tips on how to use the tools and then offered the opportunity to compete in a **Capture the Flag** event to practice those skills hands on.

In **April**, SC CIC hosted a cybersecurity training session for the **South Carolina Army National Guard's (SCARNG) 125th Cyber Protection Battalion** and the **South Carolina State Guard's Cyber Unit**. Topics covered included phishing response, malware analysis, log analysis, and leveraging threat intelligence in incident response. Attendees practiced using SC CIC's preferred security tools and completed exercises based on real events the team previously handled.



SC CIC Security Analyst Joe Taylor presenting at the guard training

In **August**, SC CIC hosted a **Java Install** at **Southeastern Freight Lines**. Java Installs, which are normally held via Microsoft Teams, are informal monthly coffee chats that give CLOs the opportunity to ask questions, network, and build relationships with other CLOs across the state. This marked the first time a Java Install was held in person, allowing participants to connect and collaborate in a new way. SC CIC will continue to host these in different locations in 2024, giving participants in all regions of the State the opportunity to attend.

Also in **August**, SC CIC began hosting regional **Elections Cyber Resource Meetings**, in partnership with the **SC State Elections Commission (SEC)**, **EI-ISAC**, and **CISA**. The goal of the Elections Cyber Resource meetings was to educate county IT and elections directors about available cybersecurity resources on a state and federal level in anticipation of the 2024 election. Over **70 county IT and elections employees participated** in the events statewide.



SC CIC Director Ryan Truskey and Katie Scroggins at an Elections Cyber Resource Meeting

In **September**, SC CIC partnered with **Panoptcy Security** to present a “**choose your own adventure**” **Tabletop Exercise (TTX)** that walked participants through critical decisions when facing a ransomware incident. Each choice made impacted the next part of the scenario, which was well-received by the audience.

In **October**, SC CIC was a featured guest at the **Strengthening Cybersecurity** summit coordinated through the **University of South Carolina (USC)** and the **Columbia Council for Internationals (CCFI)**. Security leaders from **20 countries** met for a day to exchange ideas and best practices across cybersecurity realms from investigative and legal to research and intelligence. The countries represented spanned several continents and included Barbados, Brazil, Malaysia, Morocco, Poland, Senegal, and Ukraine.

In **November**, SC CIC hosted a **regional TTX in Beaufort, SC** with the **South Coast Cyber Center** and **SCARNG**. The scenario presented a phishing email campaign that evolved into a malware incident and walked through the organizations' response as the threat evolved. SC CIC provided participants with expert guidance on the techniques and defense strategies discussed throughout the exercise and passed along key resources to help strengthen their response plans. The exercise involved **11 organizations** and **over 45 participants**.



SC CIC Cybersecurity Advisor Rick Kelly leading the Beaufort Regional TTX

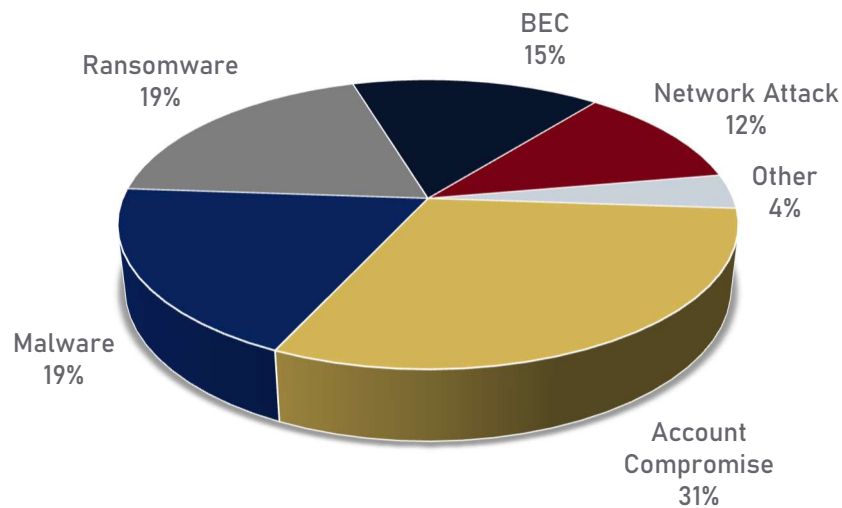
The Citadel Research Project

In 2023, **SC CIC** began collaborating with **The Citadel** on a **long-term critical infrastructure research project**. The goal of the project is for cadets majoring in Cybersecurity and Computer Sciences-related degrees to create **custom sector-specific threat profiles** for each of the 16 sectors that capture the highest risks along with recommendations to remediate those risks. Each semester, students choose the sector they are most interested in researching and are paired with CLOs working in that sector. This allows the students to get firsthand information about threats their chosen sector is facing while also facilitating a professional networking connection for the future. In the Spring of 2023, students focused their research on the **Water and Wastewater** sector, and in the Fall of 2023, the students chose the **Energy** sector. SC CIC will continue to support this project in 2024.

SC CIC and Significant Cyber Incidents

In 2023, SC CIC **responded to 27 significant cyber incidents** impacting critical infrastructure in South Carolina. The sector that experienced the **highest number of incidents in 2023** was the **government facilities** sector with **20 incidents**. They were followed by the water and wastewater sector with two incidents. It should be noted that this disparity can be partially attributed to the weighting of sectors that participate in the SC CIC program, with government facilities being the highest represented by a significant margin.

Types of Incidents in SC in 2023



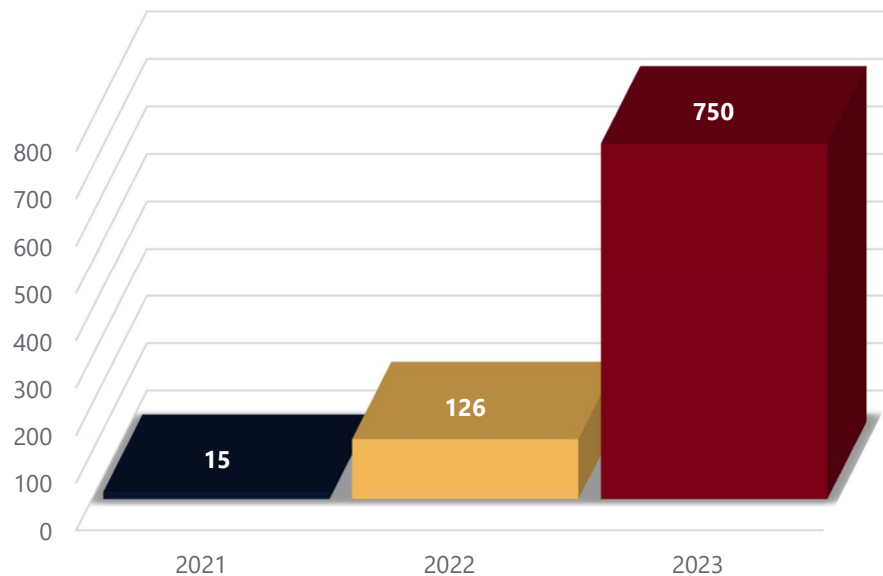
As seen in the chart above, the incident category with the **highest occurrence in SC in 2023** was **account compromise**, with malware and ransomware tied for second place. In comparison, the most frequently occurring type of incident seen last year was malware, followed closely by ransomware. Account compromise occurs when an account is accessed by a person not authorized to use it. Incidents are classified this way when credentials are stolen, such as when a user inadvertently enters them into a fake login site, or when an account is accessed with credentials obtained from an initial access broker. Ransomware is a subset of malware that involves data encryption to prevent access and an extortion demand to restore normal operations. SC CIC decided to track ransomware separately from malware as it became increasingly common over the past few years to maintain statistical clarity. **The significant increase in account compromises this year supports SC CIC's choice to put resources into both the Active Directory assessment and Phishing & Security Awareness services** as these have the best chance of protecting the state from this trending threat.

Incident Response

SC CIC's Incident Response (IR) efforts include providing incident coordination, secure out-of-band communications, cybersecurity consultation, event log analysis, and malware analysis. As the malware analysis process has been streamlined and malware analysis capabilities matured, SC CIC was able to analyze **750 files and websites** for potential malware or other malicious

intent **in 2023, which represents 495% more than the previous year.** These analyses help CLOs make determinations about potential phishing emails or malware seen in their networks and provided insight into the motives and tactics of threat actors attempting to disrupt the state's critical infrastructure networks.

SC CIC Analyses Performed by Year



In **January**, SC CIC responded to a **unique phishing campaign** that allowed threat actors to obtain initial access to a county government network. At first, it appeared to be a common campaign that uses a compromised mailbox and contact list to spread the phishing emails. Upon deeper investigation, SC CIC discovered that it was much more complicated. First, the threat actor used a reverse proxy to relay and capture credentials and multi-factor authentication (MFA) tokens. Then, once authenticated into the victim's account, the existing Microsoft Exchange **permissions were**

used to register a malicious application impersonating an app called Perfect Data Recovery to the victim's enterprise Azure environment. This would maintain access if the user's password was reset, **which is a novel form of persistence.** SC CIC created and shared a threat intelligence bulletin that detailed how this attack was carried

out and included specific Indicators of Compromise (IoCs) that could be used to hunt for the threat in other networks. Several CLOs found the rogue Perfect Data Recovery application as well as identifying other suspicious applications by following SC CIC's guidance. **All affected organizations were able to remove the malicious applications and secure their Azure application environments with no further impacts.**

"All affected organizations were able to remove the malicious applications and secure their Azure application environments with no further impacts."

In **April**, SC CIC spearheaded an incident response initiative for a county government experiencing a ransomware attack and coordinated task force attendance of the **Federal Bureau of Investigation (FBI)**, **US Secret Service**, and **SLED Computer Crimes**. While investigating the incident, SC CIC discerned that **an initial access broker successfully infiltrated the organization**, promptly selling the access to another threat actor responsible for deploying the ransomware. The attack **leveraged multiple Remote Monitoring and Management (RMM) tools**, which is a common tactic used to maintain persistence in a network, as well as a data exfiltration tool that was later correlated to a new trending threat actor tactic. SC CIC identified

“...which demonstrated SC CIC’s ability to swiftly process information during a cyber incident and translate it into actionable insights.”

the probable initial access vector by correlating the available logs on site and subsequently provided guidance to facilitate the organization's remediation efforts. Additionally, this incident generated a technical IoC bulletin and CLO call walkthrough of the TTPs **which demonstrated SC CIC’s ability to swiftly process information during a cyber incident and translate it into actionable insights.**

In **November**, SC CIC assisted with an incident involving a **water utility** and a **compromise of their Operational Technology (OT) network**. The threat actors gained access to the organization’s devices by compromising multiple Programmable Logic Controllers (PLC) that were publicly exposed to the internet and changing the user interface to display an anti-Israeli message on the screen. The threat actors claiming the incident are likely tied to an **Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated group**. SC CIC reported the incident to federal partners using a USCYBERCOM notification process titled Cyber 9-Line. This decision was based on the potential geo-political motivations claimed in the note left by the attacker, and the potential for harm that the change on the device represented. At least ten other similar incidents to the one experienced in South Carolina were reported nation-wide, with six of those victims being water utilities. As a result of these events, CISA and their partners released an advisory providing invaluable information to help protect critical infrastructure organizations across the nation.



Altered image threat actors placed on water utility monitoring devices

Also in **November**, SC CIC responded to an incident related to a city employee's email account being compromised. This victim's email account was used to send phishing emails with malicious links to other victims across the state. SC CIC quickly partnered with the victim's organization to gather information about the attack, walked them through the process of securing and fortifying the account, and analyzed the email to better understand the initial attack. With the information acquired throughout the response, **SC CIC was able to alert 101 organizations to phishing emails in their inboxes** so they could remove them before user interaction. **SC CIC also utilized its domain mitigation service to quickly take down the related credential harvesting pages.** This defense-in-depth approach to phishing has proven to be highly effective. **By combating phishing threats in multiple ways, SC CIC continues to improve the threat landscape for all South Carolinians.**

"By combating phishing threats in multiple ways, SC CIC continues to improve the threat landscape for all South Carolinians."

Services Provided

Cyber Posture Review

SC CIC's CPR is a self-assessment consisting of a short, but comprehensive, survey based upon CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)², which directly map to the NIST Cybersecurity Framework and its five functions: Identify, Protect, Detect, Respond, Recover.

After the CPGs were released at the end of 2022, **SC CIC dedicated 2023 to redesigning its existing CPR to fully align with the latest federal guidance.** This change allows SC CIC to adapt the CPR to industry best practices in real-time as the CPGs are updated while limiting the time required for participants to complete security audits since they'll already be completing the one backed by CISA. The CPR is valuable to both SC CIC and the state, in that it **allows for the possibility of metrics-based prioritization of resources, response, and mitigation efforts across South Carolina's critical infrastructure.**



The CPR is delivered through a secure web portal that participants can access at any time and save progress as needed. Once completed, a report is generated that includes a full overview of responses for year-over-year tracking, as well as a highlighted subset of issues that SC CIC recommends are addressed first, called the "Top 5 Critical". **SC CIC prioritizes these recommendations based on what would make the highest security impact for the lowest cost and complexity.** These findings are then delivered to the organization by a member of SC CIC with constructive feedback and specific recommendations for improving their security posture through both technical and non-technical means. In 2024, SC CIC will administer the CPR to organizations that were unable to complete it when they joined the program during the redesign and offer the revised CPR to those organizations that completed the previous version.

² <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

Threat Intelligence

By the end of 2023, there were **165 organizations** utilizing SC CIC threat intelligence services, which is **more than 10% growth** since last year. SC CIC has continued to curate its threat intelligence toolset and further honed its active research techniques to provide insights into the critical infrastructure threat landscape in South Carolina, both at an individual participant level and in aggregate across all sectors. The state's collective attack surface is monitored through integrated intelligence platforms and by leveraging SC CIC's access to dark web markets and restricted forums where information not readily available to the public, such as the sale of compromised network access, can be found.

One of the SC CIC threat intelligence program's greatest strengths is its proven ability to share intelligence with the appropriate audience that is timely, relevant, and concise. Participant feedback continues to indicate that it is often SC CIC that provides initial alerts regarding security threats that need attention. Various alerts and bulletins are distributed to the CLO network throughout the year and are designed to maintain awareness of the current threat landscape and latest malware observed in the wild. When warranted, these communications also detail the steps needed to mitigate actively exploited vulnerabilities. In 2023, there were **11 intelligence bulletins** disseminated to critical infrastructure participants.

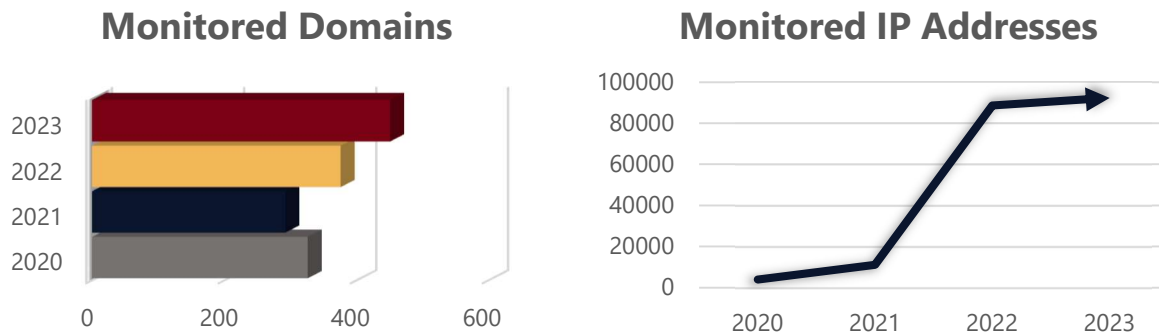
SC CIC monitors a variety of intelligence sources that host, distribute, or sell stolen credentials to alert participants if usernames and passwords associated with their organization are shared. These typically include website leaks that can be attributed to a particular breach or malware logs, which come straight from threat actor-controlled server logs of infostealer malware. This stolen data regularly ends up on dark web markets, allowing multiple cyber threat actors to purchase it and potentially use it to gain access to an organization's network or systems (also known as initial access). In total, SC CIC identified and alerted on **96 unique batches of leaked credentials in 2023**, with each batch containing anywhere from a single username and password pair up to hundreds of pairs and resulting in more than 450 alerts sent. To increase the quality of these alerts, **SC CIC considered participant feedback and decided to eliminate combo list leaked credential results from the data** sent to participants. The combo lists were typically low fidelity as they were repackaged from other leak sources and often contained errors or username password pairs that were more than a few years old.

Halfway through this year, **a new partner joined SC CIC** in the fight against stolen credentials and the ecosystem of initial access, **DarkWeb IQ**. This organization uses DOJ-approved methods of gaining clandestine access to dark web markets and

forums to monitor the sale of stolen credentials firsthand. This allows SC CIC to notify victims in the state hours, or even days, before the cyber threat actors have a chance to act. The value of the alerts from this new source was quickly proven, as **SC CIC was able to prevent an incident from escalating at a local Sheriff's Office** within the first few months. The alert showed that someone in the organization had a malware infection that had facilitated data exfiltration, which

"...SC CIC was able to prevent an incident from escalating at a local Sheriff's Office..."

was already being advertised on a dark web forum as a form of access into the victim organization's network. The stolen data would have allowed any buyer to impersonate the victim and bypass protections, such as MFA. This minor malware infection could have led to a major network event, like ransomware, but instead SC CIC made timely notification, the malware was remediated, the account secured, and there was no further impact to the victim organization.



As of the end of 2023, SC CIC is **continuously monitoring 92,356 IP addresses and 451 domains** for unintended public exposure, public-facing vulnerabilities, dark web presence, and potential compromises. This allowed SC CIC to **make 136 notifications this year about risky exposed services**. These included alerts like vulnerable Microsoft Exchange servers or risky services such as Telnet, Server Message Block (SMB), or Remote Desktop Protocol (RDP) that were enabled, exposed, and visible to the internet. Furthermore, **315 deep or dark web presence alerts** were generated. Some of these alerts are based on optical character recognition (OCR) technology matching the names and/or logos of the organizations on websites they typically should not be found such as the logo of a company showing on a fake landing page meant to trick users into logging in with their credentials.

Adversary Emulation

Adversary emulation was introduced as an SC CIC service in 2022. This is a security engagement that imitates an attack against the target organization. SC CIC leveraged its threat intel resources to create custom emulation campaigns matching current cyber-attacks seen in the wild so the organization's detection and response capabilities could be tested without the damage that accompanies a real incident. A detailed report was then provided which outlined the attack path that was taken paired with explanation and resources to better prevent, detect, and/or remediate similar attacks in the future.

In 2023, SC CIC completed adversary emulation campaigns for four different organizations. Each organization completed the campaigns more than once so that security controls could be tuned and re-tested, and/or the effectiveness of security products being used in the environment could be fully established. SC CIC was able to help every participating organization make data-driven decisions about their security products, improving both their security capability and cost efficiency or justifying budget requests.

This year, SC CIC noticed a decline in the requests for adversary emulation compared to the

prior year and uncovered that the highly technical nature of the service made it difficult for most participants. In alignment with its mission to make the largest impact on the highest number of critical infrastructure organizations in the state as possible, SC CIC shifted gears to a service that would engage participants at all levels of technical maturity, the readiness exercise.

Readiness Exercises

Cyber readiness exercises are engagements designed **to assess and improve an organization's ability to detect, respond to, and recover from various types of attacks and risks**. The purpose is much like that of adversary emulation, but the flexibility and holistic approach to their delivery is the key to serving the most SC CIC participants. Organizations are surveyed prior to an engagement to assess both what their current capabilities are and what they'd like to get out of the exercise. They are encouraged to invite multiple departments to participate (such as IT, security, legal, or executives), which facilitates collaboration and authentic conversations about how they would respond to a real threat. Because of the adaptable nature of these exercises, **they can be tailored to benefit a wide range of organizations**, from providing essential learning opportunities for novice security teams to challenging security experts with advanced simulations and attack emulations that mimic the Tactics, Techniques, and Procedures (TTPs) used by real adversaries.

After completing an exercise, participants receive a comprehensive report which includes a summary that highlights exercise objectives, major findings, and high-level recommendations for organizational leadership. There is also an analysis of the results, including an assessment of the organization's cybersecurity maturity on a

"These exercises provide SC CIC with unique insight into the security posture of critical infrastructure sectors across the state..."

scale, a breakdown of cybersecurity maturity at each phase of the incident response process, identification of specific areas where security is lacking, and recommendations on how to strengthen capabilities for each skill exercised. Each aspect of the exercise includes a score so that improvements can be objectively verified over time. **These exercises provide SC CIC with unique insight into the security posture of critical infrastructure sectors across the state**, which can help optimize security spending by directing funds where they are most needed.

SC CIC began piloting this service in Q4 of 2023 and has completed readiness exercise engagements with four organizations. Feedback has been wholly positive, and more CLOs have already expressed interest in participating. In 2024, SC CIC will offer this service to all participants.

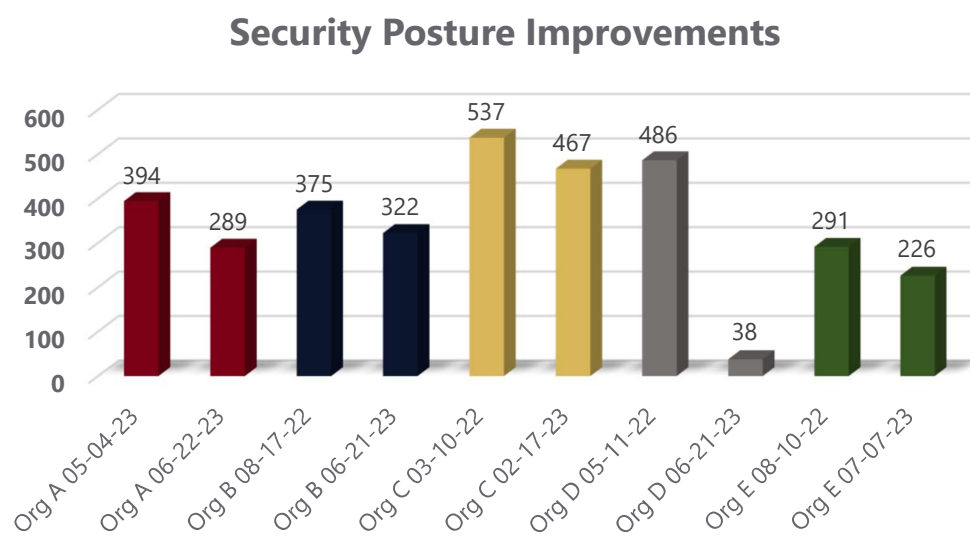
Active Directory Security Assessment

Based on observed attack trends, SC CIC developed and began offering the **Active Directory Security Assessment** in 2022. Microsoft's Active Directory (AD) is a core component of most organizations' IT environments that allows administrators to centrally manage users and access

permissions. Being a major control center for critical systems and data, attackers can leverage AD to move laterally and/or escalate privileges once a foothold is established inside a target organization's domain. These assessments help SC CIC participants **evaluate their AD security posture and provide actionable guidance to improve it.**

Utilizing tools like Bloodhound and PingCastle, SC CIC identifies vulnerable configurations and attack paths that a threat actor could use to carry out malicious activities. Participants are provided with a robust report following the engagement that details what was found, offers guidance on steps to take for remediation, and provides additional material to foster a better understanding of their environment. Additionally, a risk score is generated so that improvements can be quantified over time. These **metrics provide the SC CIC team with valuable insight into postural trends across the state and helps us better serve all participants.** SC CIC also uses this information to develop presentation material for its monthly CLO calls, thereby ensuring that the wider community is better protected.

This year, **22 organizations** participated in SC CIC's Active Directory Security Assessment service. For participants who have conducted multiple assessments, **an average improvement of 16% has been seen between the first assessment and their most recent one.** Organizations also commonly request assessments after making substantial changes to their AD environment. Interestingly, a few organizations this year had higher scores (indicating weakened posture) between the first assessment and a follow-up. This highlights **another benefit of the service, which is the identification of unintended consequences after making changes.** This information was invaluable to those organizations, serving to both deepen the internal security team's understanding of AD management and ensuring issues were corrected before they could be taken advantage of by a potential adversary. In the chart below, five organizations are anonymously represented with their initial and follow-up scores (a lower score represents a better posture).



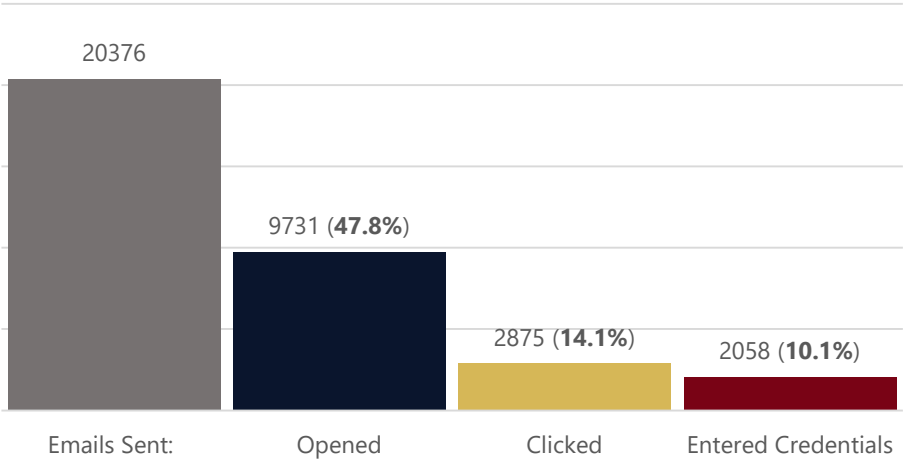
Simulated Phishing and Cybersecurity Training

Phishing continues to be one of the most common forms of attack for threat actors attempting to carry out malicious activities and SC CIC remains committed to strengthening the human layer of security among its participants. To accomplish this mission, real-world phishing emails are used to develop templates designed to test the awareness of end-users. This helps ensure that users across the state are better prepared to safely operate in the current threat landscape.

This year, SC CIC incorporated QR code phishing into a new template after it was observed as a new tactic used by threat actors in the wild, demonstrating the dedication to relevancy and delivering the most impactful product possible.

In 2023, 26 organizations utilized the phishing program, with six of those doing so for the first time. In total, **20,376 simulated phishing emails** were sent out to participating organizations resulting in **47.8% of the users opening the email** which led to **14.1% of users clicking on links** and **10.1% entering credentials into fake login portals**.

Results of 2023 Phishing Campaigns



Both clicks and credentials entered increased since last year, which is likely a byproduct of the improvement in templates used to test users. The most effective phishing template was a fake Office 365 Outlook login landing page, something users encounter daily during normal work operations. After each phishing campaign, SC CIC provides training courses designed to improve the users’ ability to detect phishing emails in the future. **In 2023, SC CIC delivered training material via 3,051 emails to improve security awareness** and empower end users with the knowledge to better serve as the last line of defense for their critical infrastructure organization.

In addition to offering phishing tests and training, **SC CIC actively neutralizes the malicious web pages that support the attacker’s campaigns**. Phishing attacks frequently employ web pages that mimic legitimate login portals, enabling attackers to harvest user credentials. When an unsuspecting user attempts to log in, the threat actors intercept the credentials, using them to access the network and launch subsequent attacks. When one of these pages is identified, SC

CIC collaborates with its partners to quickly deactivate the site. With the malicious site disabled, corresponding links in the phishing emails become harmless since they will no longer direct end users to the credential-harvesting page. By preventing the extraction of credentials from these malicious pages, SC CIC significantly impedes the spread of attacks within South Carolina and beyond.

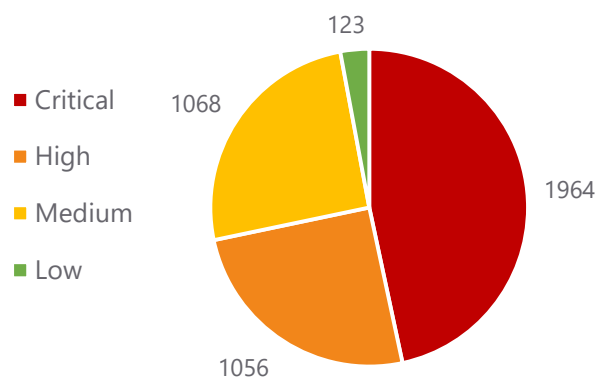
Throughout 2023, **SC CIC successfully deactivated 64 malicious websites** used in such attacks and **notified 29 organizations of compromised accounts** within their systems. This allowed the affected organizations to swiftly respond and secure the accounts, preventing further impacts. Given the nature and rapid spread of phishing attacks, combatting them necessitates the multi-pronged approach SC CIC has developed. This includes comprehensive user training, rapid attack identification, quick account recovery, aiding organizations in recovering compromised accounts, and fortifying their account security.

Vulnerability Scanning

SC CIC delivers external vulnerability scanning as a service by leveraging Nessus through Tenable cloud scanners to provide an outside perspective of the organization's internet-facing assets. **This mimics what a potential attacker would see and gives valuable insight into a common initial network access vector.** An SC CIC analyst then reviews each scan result to create a succinct personalized report with recommendations for remediation based on probability of exploitation and expected impact. On-demand verification scans are also performed once fixes are implemented to ensure that security gaps are closed.

SC CIC has been able to provide **108 organizations** with vulnerability scanning, an increase of 25 from last year, and discovered **4,211 vulnerabilities** in 2023. The most common vulnerability seen this year involved deprecated versions of Transport Layer Security (TLS) being enabled on servers. TLS 1.0 and 1.1 were formally deprecated in 2021 and having them available makes the server potentially susceptible to a downgrade attack where the lesser protocol would be used and leveraged to exploit the host. These are easily remedied by disabling the protocols and represent an easy win for SC CIC in improving South Carolina's public security exposure.

Vulnerabilities Discovered by Severity



Conclusion

SC CIC has thrived in 2023 with its innovative model of adaptive cybersecurity service delivery combined with nurturing its invaluable network of CLOs and partners across the state of South Carolina. This year's highlights include the implementation and delivery of readiness exercises that test organizational resilience from the basic security planning stages up through hands-on technical incident response practice, streamlining leaked credential notifications by eliminating low fidelity sources, developing a new QR code simulated phishing campaign, and acquiring a new malware analysis tool which significantly improved analysis speed and quality. The SC CIC team remains alert to the changing needs of the state and will adjust course whenever a new challenge presents itself. Maintaining SC CIC's resilience and agility while expanding the team to continue supporting as much of the critical infrastructure in the state as possible remains a core goal in the future.

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: A Microsoft directory service for the management of identities in Windows domain networks.

Azure: Microsoft's public cloud computing platform.

Business Email Compromise (BEC): A specific type of phishing attack designed to trick employees into taking harmful actions, typically sending money to the attacker.

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".

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

Cortex XDR: A Palo Alto XDR product; see XDR.

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.

Cyber 9-Line: A template of questions used to quickly communicate a cyber incident to USCYBERCOM that operates similarly to the military reporting used by battlefield medics to report combat injuries quickly and accurately while in the field.

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

DarkWeb IQ: A public-private partnership that coordinates with the law enforcement community and insurance industry to serve as an early warning system that enables companies to fight against ransomware.

Defense-in-Depth: A cybersecurity approach in which a series of security mechanisms and controls are layered throughout a computer network to protect the network and the data within so that mitigations are in place against a wide variety of threats and redundancy exists in the event one mechanism fails.

Domain Mitigation: A term for the various tactics used in dealing with problematic websites

such as those hosting malware or pretending to be a legitimate site.

EI-ISAC: “Elections Infrastructure Information Sharing and Analysis Center”; a voluntary, collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government Coordinating Council (GCC) working to ensure the integrity of elections among U.S. State, Local, Tribal, and Territorial (SLTT) governments.

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.

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.

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

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.

NIST: “National Institute of Standards and Technology”; an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

Operational Technology (OT): A term that refers to devices that interface with the physical world and the hardware or software that controls or monitors the equipment. Examples include automated lighting, HVAC, or fire control systems, and industrial machinery.

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.

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.

Programmable Logic Controller (PLC): A computer system that is used to automate processes that require precise and repetitive control, such as monitoring temperature, pressure, and other variables. PLCs are widely used in various critical infrastructure sectors such as the Chemical, Critical Manufacturing, Energy, and Water and Wastewater Systems sectors.

QR Code: "Quick Response"; a type of barcode that stores information and can be read by a digital device, such as a cell phone.

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.

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.

Remote Monitoring and Management (RMM): A set of tools and software used by IT professionals to remotely monitor, manage, and maintain IT systems and networks.

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

SOAR: "Security Orchestration, Automation and Response"; a software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows while automating repetitive tasks.

Soteria: Cybersecurity service provider in South Carolina that offers advisory, consulting, and incident response assistance to clients.

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.

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.

Transport Layer Security (TLS): A cryptographic protocol that protects internet communications.

USCYBERCOM: One of the 11 unified combatant commands of the United States Department of Defense which unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise which focus on securing cyberspace.

XDR: "eXtended Detection and Response"; a consolidation of tools and data that provides extended visibility, analysis, and response across endpoints, workloads, users, and networks.

XSOAR: A Palo Alto SOAR product; see SOAR.