South Carolina Critical Infrastructure Cybersecurity

2024

Year in Review

Table of Contents

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.

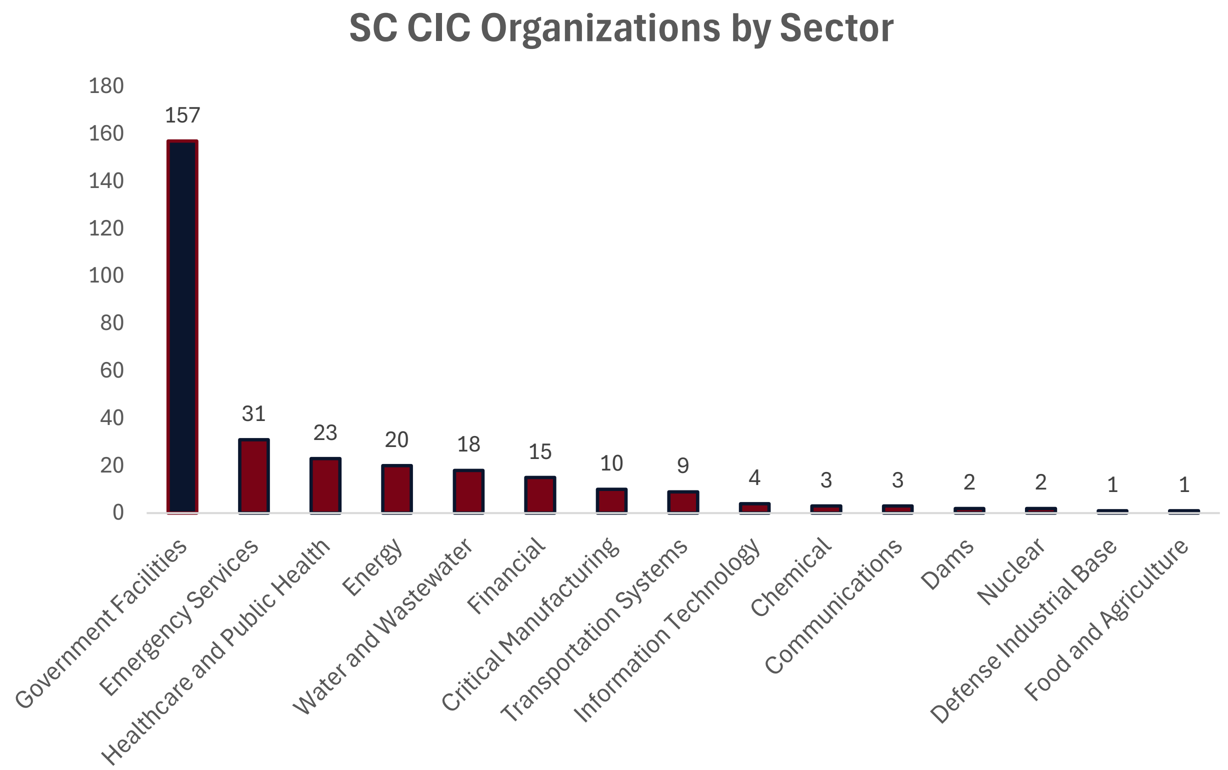
SC CIC services include threat intelligence, readiness exercises, Active Directory (AD) assessments, phishing and security awareness training, and vulnerability scanning. These services have been thoughtfully chosen with the aim of making the biggest possible impact on the cybersecurity posture of the 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 2024.

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. In 2024, state funding was secured that will allow SC CIC to expand in more commensurate response to the growth and demonstrable cybersecurity needs in the state. This expansion will allow the team to refine its services, reach an even wider audience, and spend more time with each individual organization.

SC CIC Overall Growth

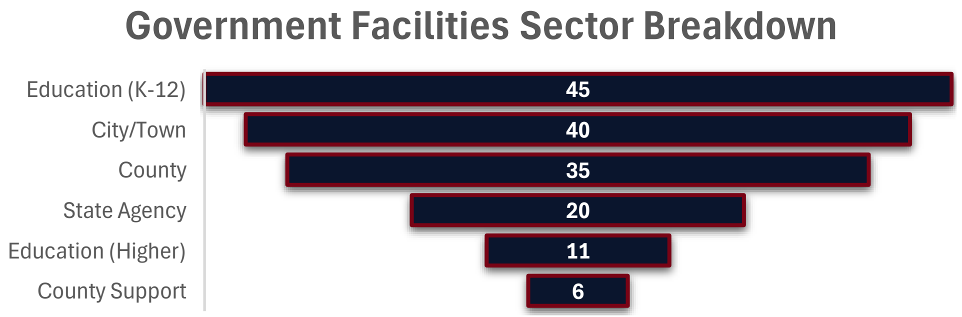
In 2024, the total number of SC CIC organizations grew to **279**, an increase of **32** from the previous year. These organizations represent **15 out of the 16 critical infrastructure sectors** identified by Presidential Policy Directive 21 (PPD-21)[1] as **SC CIC welcomed its first Food and Agriculture Sector participant this year**. The sector not represented is Commercial Facilities. While SC CIC services could be offered to this sector, a cyberattack against it is more likely to lead to financial losses rather than halting essential services, so they will be considered on a case-by-case basis. Continuing the trend seen in previous years, **Government Facilities is the most represented 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 sustained growth of new organization participants in 2024 attests to the power of relationship building and the networking success of SC CIC, its participants, and partners across the state.



It should be noted that some organizations fall under multiple critical infrastructure sectors so the sum of the columns in the SC CIC Organizations by Sector chart is higher than the total number of participating organizations in SC CIC.

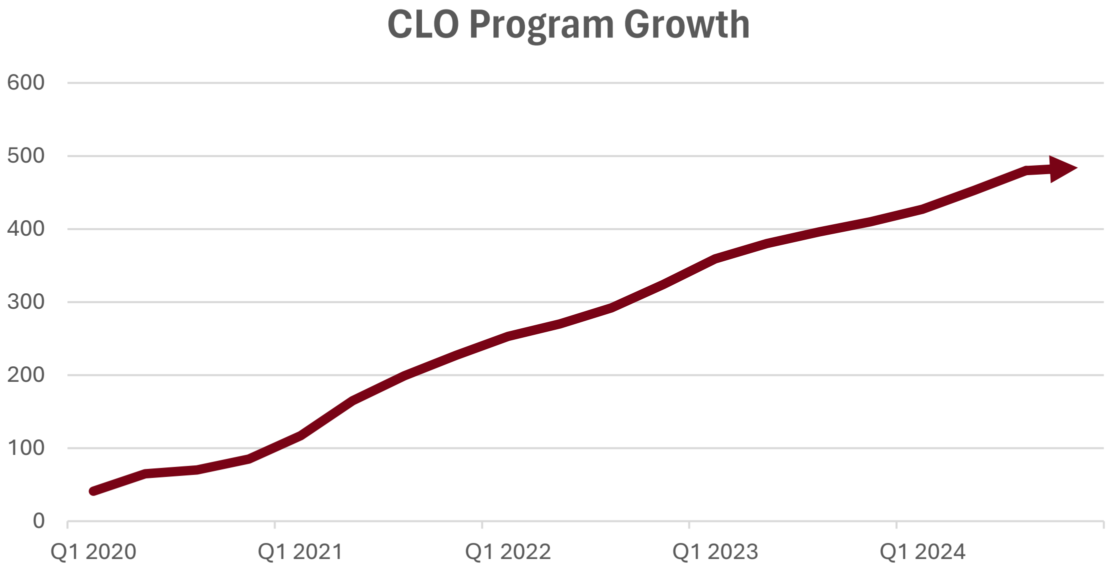
[1] https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and

The Government Facilities Sector is comprised of local and state government, plus the Education Facilities and Elections Infrastructure Subsectors. The elections category typically aligns with County-level government. The following graph further categorizes the 131 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 higher education institutions. The County-Level Support category represents agencies that operate at the county level, such as solicitor's offices.



Cyber Liaison Officer Program

Cyber Liaison Officers (CLOs) are a key pillar of SC CIC. CLOs are IT professionals and administrators who coordinate their organization's onboarding into SC CIC, identify which services to engage, and then participate in events to bring lessons learned back to their daily work. **CLOs serve as the primary point of contact, playing an integral role in the threat intelligence ecosystem facilitated by SC CIC in the state**. This two-way information sharing ensures that relevant cyber threats, incidents, and trends seen in South Carolina critical infrastructure environments are swiftly communicated to those who need it. **At the end of 2024, the total number of SC CIC CLOs was 485**, an increase of 75 from 2023.



CLO Calls

SC CIC hosts monthly calls to keep the CLO network updated and to facilitate regular communication between participants and the team. 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 **Recorded Future** covering ransomware and how recent threat actor takedowns affected the overall ecosystem
- A presentation of the unique port and maritime cybersecurity challenges and considerations from a CLO at the **South Carolina Ports Authority**
- An overview of election security in South Carolina and the proactive steps the state takes to prepare for its elections led by the **South Carolina Election Commission (SEC)** and SC CIC's Elections Security Advisor
- A technical walkthrough of email security challenges and potential solutions from a CLO at **Southeastern Freight Lines (SEFL)**
- A panel discussion featuring multiple CLOs about the success and impact of SC CIC's Readiness Exercises

External Engagements

SC CIC connects and builds relationships with critical infrastructure organizations in South Carolina through regular external engagements. These opportunities foster information sharing with the security community and provide invaluable insight into the state's current cybersecurity challenges. In 2024, SC CIC personnel were invited to participate in **20 events** that included presenting at:

- The **SC Rural Water Association Decision Makers Summit**
- The **SC Association of School Administrators (SCASA) Technology Leaders' Roundtable Meeting**
- **Clemson University's Collaborative CMMC Certification & Cybersecurity Seminar**
- The **Electric Cooperatives of South Carolina IT Group Conference**
- The **SC Association of Counties (SCAC) Annual Conference**

SC CIC Program Coordinator Katie Scroggins at annual SC Rural Water Association summit

SC CIC also hosts its own events throughout the year. Each month, informal meetings called **SC CIC Office Hours** are held that give CLOs the opportunity to ask questions, network, and build relationships with other CLOs across the state. These are normally conducted virtually via Microsoft Teams. This year, with workforce development in mind, SC CIC hosted the first in-person Office Hours events at **North Greenville University (NGU)** and **Trident Technical College (TTC)**. These events brought cybersecurity students together with CLOs and the team to learn about working in the field firsthand and to practice essential networking skills. They were an immense success, and **SC CIC will continue to partner with higher education institutions across South Carolina in 2025 to continue forging strong connections with college graduates and potential future employers in the state**.

SC CIC at North Greenville University

SC CIC at Trident Technical College

In **August,** SC CIC partnered with **Google** and **Microsoft** to facilitate **Conditional Access (CA) Workshops**. The team identified this need through an observed uptick in incidents involving account compromise and conversations with the CLOs handling them. During these workshops, Microsoft and Google engineers provided a comprehensive demonstration of configuring CA policies according to the recommended best practice for each type of environment. CLOs also had the opportunity to ask questions directly, learn more about how different threats can be mitigated through these policies, and follow along with a hands-on walkthrough of deploying them.

In **October**, SC CIC hosted a **South Carolina Water Cyber War Games** event in West Columbia, SC. This event was coordinated in response to the recent efforts by the **U.S. Environmental Protection Agency (EPA)** to encourage water and wastewater facilities to improve their cybersecurity posture. The event immersed participants in realistic scenarios that tested cyber incident response capabilities and facilitated conversations between key critical infrastructure organizations in the state. **Participants included representatives from 25 South Carolina water and wastewater facilities, electric cooperatives, and local municipalities.**

South Carolina Water Cyber War Games event

Election Security

SC CIC and the **South Carolina Election Commission (SEC)** work closely to ensure the safety and security of elections in the state. The SEC is also a part of the SC CIC Task Force, whose members can be engaged in the event of an election incident, ensuring swift response and resolution.

Through this partnership this year, SC CIC:

- Conducted **regional workshops across the state leading up to the Presidential Election** to inform key elections staff and leadership about security resources and eligibility. Representatives from Cybersecurity and Infrastructure Security Agency (CISA) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) were invited to speak about federal resources and answer questions, ensuring that attendees left with actionable next steps.
- Hosted an **Election Day Command Post with SC CIC Task Force** representatives from Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), CISA, South Carolina Army National Guard (SCARNG), and the SC Department of Administration in attendance. Additionally, **the SC CIC Election Security Advisor spent the day at the SEC** to ensure swift communication and response to any issues. SC CIC hosted a situational awareness chat room that was available from poll open to close, then kept in contact with the SEC until county vote reporting was called complete for the night.
- Worked alongside the SEC to help **identify and facilitate grants for** offices that needed **security upgrades** such as power generators and security camera systems. These grant projects are ongoing.
- Assisted the SEC with **data analysis of security assessments** done for the counties to identify a potential need for an Incident Response Framework Workshop that SC CIC will help coordinate and facilitate in the future.

These efforts illustrate the strength of the alliance established in South Carolina through SC CIC and its state and federal partners. SC CIC looks forward to continuing to build and develop these partnerships to protect the state's elections in the future.

The Citadel Research Project

In 2024, SC CIC continued to partner with The Citadel on a **long-term critical infrastructure research project**. The project's goal is for cadets majoring in Cybersecurity and Computer Sciences-related degrees **to create custom sector-specific threat profiles for each of the 16 critical infrastructure sectors** that capture the highest risks each one is likely to face along with recommendations to remediate those risks. Each semester, students collaborate with SC CIC to select a relevant sector to research and are then paired with CLOs working in that sector. This allows the students to get firsthand information about threats the chosen sector is facing while also facilitating a professional networking connection for the future. In the **spring of 2024**, students focused their research on the **Nuclear Materials, Reactors, and Waste Sector**, and in the **fall of 2024**, the students chose the **Transportation Systems Sector**. SC CIC aims to expand this project in 2025 to partner with other higher education institutions.

2024 SC CIC Conference

In August, SC CIC hosted its inaugural cybersecurity conference in West Columbia, SC. More than **75 CLOs** attended the event. Opened by **South Carolina Governor Henry McMaster** and **SC Law**

Enforcement Division (SLED) Chief Mark Keel, the SC CIC conference featured speakers such as Gerry Auger from Simply Cyber, Andrew Morris from GreyNoise, and Allan Liska from Recorded Future covering topics which included ransomware, Industrial Control Systems (ICS) security, law enforcement impact, and innovative ways to combat malicious internet traffic.

SC CIC team members delivering opening remarks for the inaugural conference

Additionally, several **workshops were offered**, including **Building an Incident Response (IR) Plan**, led by Brandon Poole of Panoptcy Security, and **Triaging Indicators of Compromise**, facilitated by Cory Nance and TJ Nelson of Recorded Future. Elastic also hosted a **Capture the Flag (CTF)** event for conference participants throughout the day.

The SC CIC Conference gives participants the opportunity to network and exchange ideas with fellow CLOs and other cybersecurity experts. SC CIC received wholly positive feedback from the attendees and plans to host another conference in 2025.

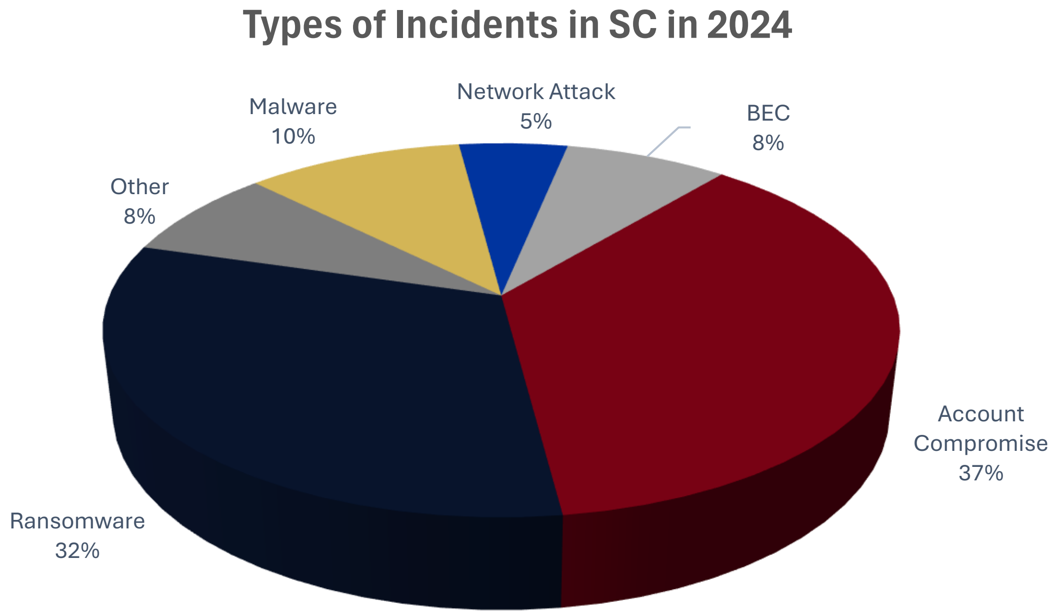
Mike Holcomb & Tim Otis during the 2024 SC CIC Conference ICS Cybersecurity fireside chat

CLOs participating in the 2024 SC CIC Conference Elastic CTF event

SLED Chief Mark Keel, SC CIC Director Ryan Truskey, and SC Governor Henry McMaster

SC CIC and Significant Cyber Incidents

In 2024, SC CIC **responded to 38 significant cyber incidents** impacting critical infrastructure in South Carolina. The sector that experienced the **highest number of incidents in 2024** was the **Government Facilities Sector** with **22 incidents**. This was followed up by the Emergency Services and Energy sectors with three and four incidents respectively. It should be noted that this disparity can be partially attributed to the weighting of sector participation in SC CIC, since government facilities continue to be the highest-represented sector.



As seen in the chart above, the **most common type of incident in South Carolina in 2024 was account compromise**. This continuing trend was first observed last year as identified in the 2023 SC CIC End of Year Report. Account compromise is a form of attack that allows threat actors to gain unauthorized access to a valid account for the purpose of initial access, persistence, privilege escalation, or defense evasion. Threat actors can gain access to accounts through means such as users unknowingly entering their credentials into a malicious login webpage after clicking a link within a phishing email. Both the AD Security Assessment and Phishing & Security Awareness services that SC CIC offers help mitigate the risks of account compromise, validating the decisions to continue devoting resources to them.

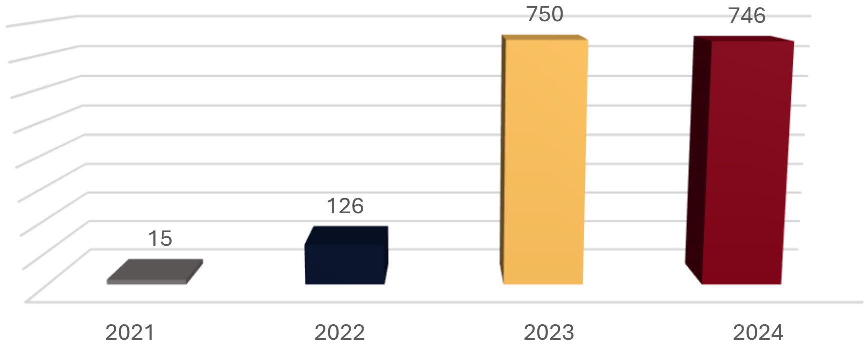
The **second most common incident encountered this year was ransomware**, a subset of malware that leverages data encryption to prevent system access and interrupt the availability of network resources. Due to ransomware's prevalence and potentially devastating effects, SC CIC tracks it separately from 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 become 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. **SC CIC is proactive in identifying potential ransomware victims** by monitoring posts in the deep and dark web for proof of network access and samples of stolen data. If a potential victim is identified in the state, the team makes out-of-band contact to help verify and respond. On multiple occasions, **SC CIC makes notification before exfiltration has been completed and before encryption has taken place, giving South Carolina organizations the opportunity to mitigate significant damage**.

"…SC CIC makes notification before exfiltration has been completed and before encryption has taken place, giving South Carolina organizations the opportunity to mitigate significant damage."

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 746 files and websites** for potential malware or other malicious intent, which represents a slight decrease from the previous year. **This decrease can be attributed to the offloading of SLED-submitted sample analysis to the newly established internal security team**, which is part of an ongoing effort to allow SC CIC staff to put full focus on external organizations. Removing these from the data set approximately offset the expected increase in SC CIC organization-submitted samples, and the upward trend is expected to resume next year. **The results of these analyses help CLOs make determinations about potential phishing emails or malware seen in their networks, providing insight into the motives and tactics of threat actors attempting to disrupt the state's critical infrastructure networks**.

Analyses Performed by Year



In February, **SC CIC responded to an account compromise** incident where an organizational email account was used to send phishing emails to the user's contacts that contained a link to a fake login site attempting to lure victims into entering their credentials. However, when the organization reset the user's password and signed all existing sessions out, the emails continued. Upon further investigation, SC CIC found that the threat actor was continuing to log in with valid credentials combined with legitimate Multi-Factor Authentication (MFA). **This aligned with an attack SC CIC has seen previously that leverages a reverse proxy to capture session tokens from the user logging in legitimately**. This adversary-in-the-middle attack allows the threat actor to appear as the victim, evading detection. The victim's account was then used to register a new device to the enterprise Azure environment, a tactic the team had not seen before. Fortunately, **the organization had already followed guidance sent out by SC CIC in 2023 that thwarted the**

threat actor's attempt to register a new application, and malicious activity ceased after this failure. The account was secured, the credential harvesting page taken down, and the organization had no further impacts.

In the same month**, SC CIC assisted a local school district with a ransomware attack**. Threat actors had encrypted an old file server that was not currently being utilized by the organization, but the server contained Personally Identifiable Information (PII), and the organization was concerned about potential compromise of that data. **SC CIC obtained and analyzed the encryption executable "xinfecter.exe" to provide threat intelligence** that included common tactics, techniques, and procedures (TTPs) and potential indicators of compromise (IOCs). SC CIC worked with the organization to use these as a guide and confirm that no exfiltration had taken place. There were no malicious tools present within the environment and no evidence of exfiltration in network traffic logs. With that knowledge, IT staff was able to move forward to remediating the gap in visibility of the old server and securing it properly.

In July, **SC CIC and several SC CIC Task Force members**, including the SC National Guard and the FBI, **responded to a ransomware attack impacting a law enforcement agency**. Evidence suggested threat actors were using **Embargo ransomware** and had exfiltrated data from the organization. Unfortunately, the organization lacked sufficient logging configurations to determine the initial access vector with certainty, but SC CIC identified an end-of-life firewall and lack of Virtual Private Network (VPN) MFA as potential avenues. Remote Desktop Protocol (RDP) was leveraged to access the organization's servers and domain controllers prior to encrypting the network. During this response effort, neighboring SC CIC participant organizations offered additional resources to assist the impacted organization. **This collaboration between SC CIC, its task force, and its participants exemplifies the overall SC CIC mission and the success of the CLO program in creating a supportive security community in the state.** This incident also prompted a CLO call walkthrough of the incident's TTPs, illustrating SC CIC's ability to process incident information and translate it into actionable guidance that can be implemented across all critical infrastructure sectors in the state.

> ***"This collaboration between SC CIC, its task force, and its participants exemplifies the overall SC CIC mission and the success of the CLO program in creating a supportive security community in the state."***

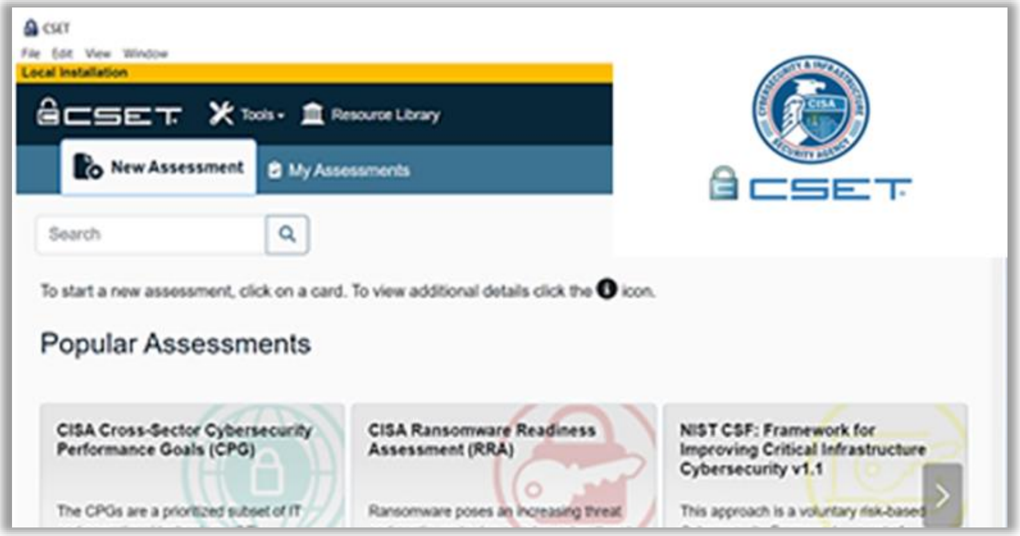
In October, SC CIC was notified by a different law enforcement agency that **a stale VPN account was used to access their network without authorization**. The organization's Endpoint Detection and Response (EDR) tool prevented the attempted installation of the remote access tool RemoteExec on a secondary endpoint, which alerted them to the malicious activity. However, a cloud storage and backup tool called BackBlaze had already been installed and used to exfiltrate files from the server, which prompted them to call SC CIC for assistance. Further investigation revealed that the compromised account did not have MFA configured, which allowed the threat actor to perform a simple brute force attack to make the VPN connection. SC CIC provided guidance on securing the network, which included a double reset of the Kerberos Ticket Granting Ticket (KRBTGT), a crucial component of securing a compromised AD environment. **This availability of on demand security expertise serves as a prime example of the value SC CIC brings to the state's critical infrastructure entities**.

Services Provided

Cyber Posture Review Sunset

In 2024, SC CIC made the strategic decision to discontinue the Cyber Posture Review (CPR) service and instead recommends that organizations adopt CISA's Cybersecurity Self-Evaluation Tool (CSET). Although delivering the CPR as a service was a success, it was also identified as a potential duplication of efforts. The CSET mirrors the functionalities of the CPR while also suggesting resources at the federal level tailored to specific critical infrastructure industries. It provides organizations with a comprehensive toolkit for self-assessment, leveraging the Cybersecurity Performance Goals (CPGs) and other cybersecurity frameworks to support the results.

To facilitate the transition, SC CIC collaborated with CISA to produce a video tutorial for participants that guides organizations through the CSET. The video covers locating and downloading the tool, setting it up, conducting self-evaluations, and establishing a regular cadence for assessing cyber environments. This shift ensures that participants have access to a robust and versatile toolset for improving cybersecurity resilience while aligning with federal best practices.



To start a new assessment, click on a card. To view additional details click the ❶ icon.

Popular Assessments

CISA Cross-Sector Cybersecurity Performance Goals (CPG)

The CPGs are a prioritized subset of IT

CISA Ransomware Readiness Assessment (RRA)

Ransomware poses an increasing threat

NIST CSF: Framework for Improving Critical Infrastructure Cybersecurity v1.1

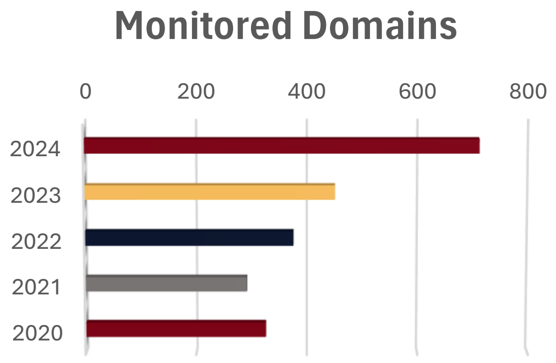
This approach is a voluntary risk-based

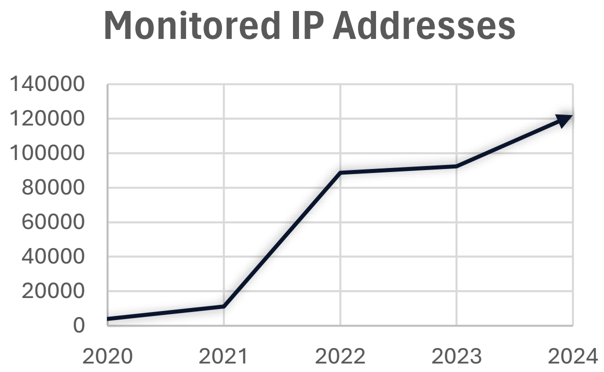
Threat Intelligence

There were **205 organizations** utilizing SC CIC threat intelligence services at the end of 2024, which is **more than 20% growth** since last year. SC CIC has continued to curate its threat intelligence toolset and further refine 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 unique access to dark web markets and restricted forums where information not readily available to the public, such as the illicit 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. Alerts and bulletins are distributed to the CLO network throughout the year and are designed to maintain awareness of the current threat landscape and the latest malware observed in the wild. When warranted, these communications also detail the specific steps needed to mitigate actively exploited vulnerabilities.

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 specific breach, or malware logs, which come from threat actor-controlled servers collecting results from infostealer malware. This stolen data frequently 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 2024, SC CIC **identified and shared more than 123 unique batches of leaked credentials**, with each batch containing anywhere from a single username and password pair up to hundreds of pairs. Compared with last year's data, that marks a 25% increase. Factoring in the overall growth in threat intelligence monitoring, the alerts outpaced that growth by 5%. This finding aligns with cybersecurity industry reports of an increasing trend of cyber threat actors acquiring valid accounts. Altogether, SC CIC's leaked credential monitoring resulted in **more than 572 high fidelity alerts being sent to participants in 2024**.





By the end of 2024, SC CIC was also **continuously monitoring 122,027 IP addresses and 710 domains** for unintended public exposure, public-facing vulnerabilities, dark web presence, and potential compromises. This allowed SC CIC to make **118 notifications this year about risky exposed services.** These included alerts corresponding to 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. Some of these exposures also affected entities outside the scope of SC CIC, such as those in other states, highlighting the interconnected nature of critical infrastructure. SC CIC endeavors to pass these on to appropriate partners when they occur. Furthermore, **597 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.

Readiness Exercises

After successfully piloting the service last year, **SC CIC started offering Readiness Exercises to all participants in 2024**. These exercises are interactive engagements designed to assess and improve an organization's ability to detect, respond to, and recover from various types of threats. They are like traditional tabletop exercises (TTXs) but with the added benefit of a centralized tracking system and enhancements such as integrated tests of technical capabilities. Scenarios are presented to participants that **simulate real-world cyber threats and challenges**, allowing teams to test existing incident response plans, identify weaknesses, and improve procedures to better handle real threats. They can also be delivered as more technical, including command injections to emulate real-world threat actors. **This combination of procedural and technical validation creates robust and adaptable exercises that test the key aspects of incident response that lead to effective recovery from attacks.** These exercises also encourage collaboration among different departments within the organization, improving reaction time while promoting a holistic and synchronized response to real cyber incidents. **Readiness exercises can be tailored to benefit a wide range of organizations**, from providing essential learning opportunities for novice security teams to challenging security experts by emulating advanced threat actors.

> ***"This combination of procedural and technical validation creates robust and adaptable exercises that test the key aspects of incident response that lead to effective recovery from attacks."***

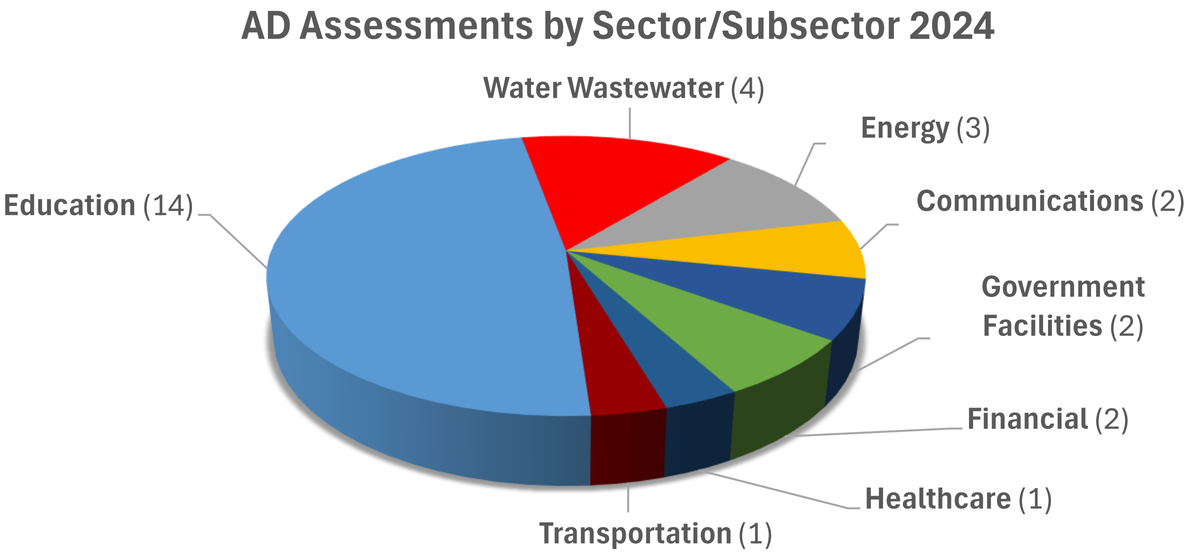
After the exercise is completed, participants receive a comprehensive report that includes an Executive Summary to highlight exercise objectives, major findings, and high-level recommendations for organizational leadership. The report also includes an analysis of exercise results, including a rating of the organization's cybersecurity maturity, a breakdown of 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. **These engagements give SC CIC unique visibility into the environments of critical infrastructure organizations across the state** to help make informed decisions about where to utilize state and federal funding to improve the security posture of these entities in South Carolina.

In 2024, SC CIC completed readiness exercise engagements with 16 organizations. The majority of these (9) were focused on building and/or enhancing incident response policies, plans, and playbooks. This approach established a solid foundation for those participants that will be built upon through additional engagements to test those plans in more advanced scenarios. This type of iterative use case is ideal for demonstrating success in the delivery of the service. For participants that incorporated technical emulations into their exercises, the value was in testing existing security tools and validating that detections and mitigations were working as expected. In some cases, alert tuning was needed to improve visibility and logging of specific threat actor techniques. Additionally, **one organization identified a gap in response from a Managed Security Service Provider (MSSP) and were able to leverage the Readiness Exercise results to amend the Service Level Agreement (SLA)**. These demonstrable successes provide evidence that SC CIC's decision to pivot to this service was the correct choice.

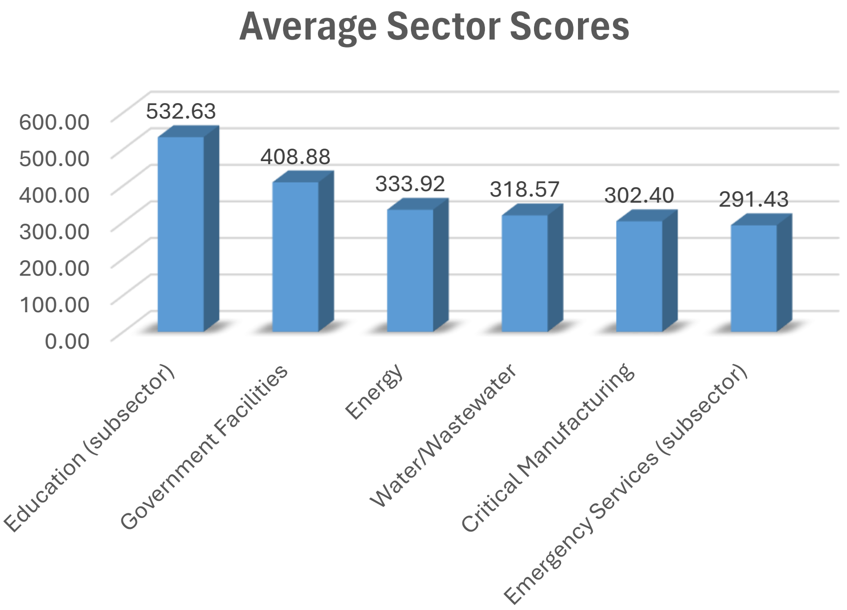
Active Directory Security Assessment

Microsoft's **Active Directory is the most widely used authentication and authorization solution in enterprise IT networks globally**. AD's prevalence across infrastructure landscapes along with the critical services it provides make it a **frequent target for threat actors seeking to carry out malicious activities**. In alignment with its overall mission to secure critical infrastructure, SC CIC developed the AD Security Assessment service to help participants better secure this important attack surface. **The goal of this assessment is to help participants evaluate their AD security posture and provide actionable guidance** to help reduce the risk and impact associated with a security incident.

During an AD assessment, SC CIC uses tools to query the target organization's AD environment and identify vulnerabilities, misconfigurations, and attack paths that a threat actor could use to carry out malicious activities. Participants are then provided with a report that details the findings, offers guidance on remediation, and provides additional material to foster a better understanding of the environment. SC CIC security analysts are also available as needed for consultation that can provide further insight and clarity for SC CIC's CLOs. Additionally, **a risk score is generated so that improvements can be quantified over time**. Each assessment finding adds to the total score, so a lower score is indicative of a stronger posture. These metrics **give the SC CIC team valuable insight into postural trends across individual sectors and subsectors, as well as the overall state**, enabling better support for all participants.



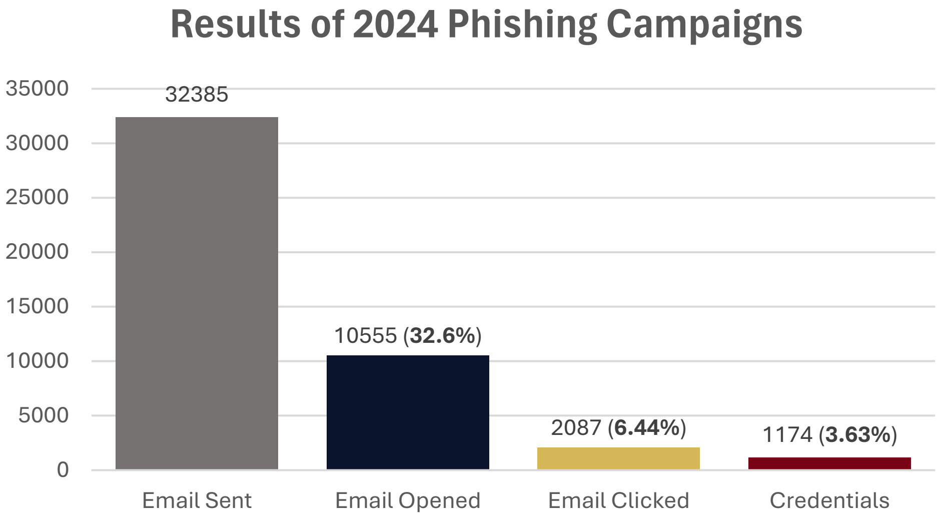
In total, **SC CIC completed 29 AD assessments this year, for 27 different organizations**. As illustrated in the chart below, **the Education subsector has the highest average score** across those that have completed an AD assessment, **and a high score indicates more security issues were identified**. However, it should be noted that as this trend became apparent, SC CIC encouraged additional organizations in that subsector to conduct assessments so improvements could be recommended to the organizations that may need it most. Because of this, almost half of the assessments done in 2024 were for organizations in the Education subsector. **The sample sizes are currently too small to make conclusions about the state of AD security across all sectors**. For participants who have conducted multiple assessments, an average improvement of 26.5% was seen between the first assessment and their most recent one this year.



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 users across the state are better prepared to safely operate in the current threat landscape. **This year, SC CIC created an OpenAI template that aligned with the recent explosion of AI used in business applications** and offered back to school templates during August and September, demonstrating the dedication to relevancy and delivering the most impactful product possible.

In 2024, 26 organizations utilized the phishing program, with 18 of those doing so for the first time. In total, **32,385 simulated phishing emails** were sent out to participating organizations resulting in **32.6% of the users opening the email** which led to **6.44% of users clicking on links** and **3.63% entering credentials into fake login portals**.



Both clicks and credentials entered decreased since last year (down from 14.1% clicked and 10.1% entered). The same fake Office 365 Outlook login landing page that was most effective last year continues to be the one that users tend to fall for, which makes sense as it mimics something they regularly encounter in normal work environments. After each phishing campaign, SC CIC offers training courses designed to improve the users' ability to detect phishing emails in the future. **In 2024, SC CIC delivered training material via 1,273 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. The training delivery frequency of this service has decreased this year as organizations implement their own phishing and security awareness programs, which is a win for sustained security improvement in the state.

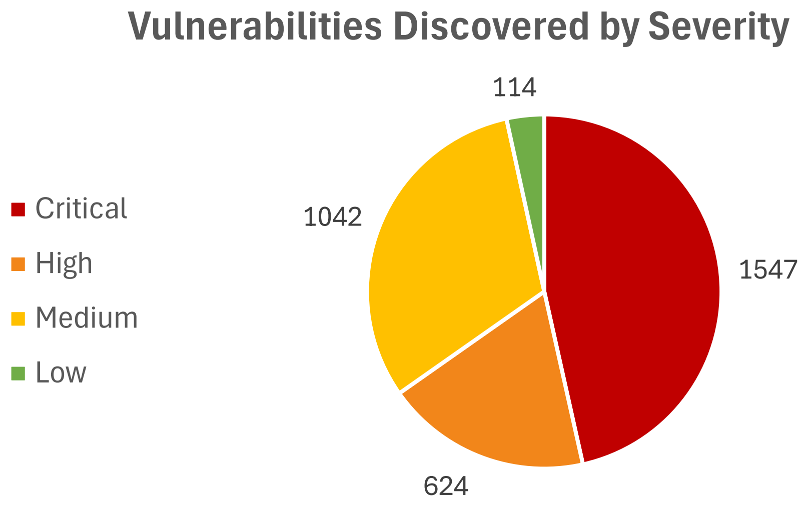
In addition to offering phishing tests and training, **SC CIC actively neutralizes the malicious web pages that support the attacker's campaigns**. Phishing attacks frequently employ web pages that mimic legitimate login portals, enabling attackers to harvest user credentials. When an unsuspecting user 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.**

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

Throughout 2024, **SC CIC successfully deactivated 134 malicious websites** used in such attacks and **notified 23 organizations of compromised accounts** within their systems. This allowed the affected organizations to swiftly respond and secure the accounts, preventing further impacts. For reference, the number of sites taken down is up from 64 last year but the number of organizations associated with compromised accounts in the state is down from 29. **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, providing aid to organizations in recovering compromised accounts, and fortifying overall 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 provided **140 organizations** with vulnerability scanning, an increase of 32 from last year, and discovered **3,327 vulnerabilities** in 2024. A common vulnerability seen this year involved untrusted certificates on edge appliances such as web and VPN servers. A certificate validates the identity of the server and allows for a secure connection to be made with others. Appliances are typically sold with a default certificate that is fine for use internally but can cause issues once the appliance is exposed to the Internet. An example of this is when a user connects to a website with a web browser and receives an error message that the site is untrusted or insecure. That is usually a certificate error. Resolving these errors ensures that data transmitted with the server is protected, which serves to better secure both critical infrastructure and citizens accessing those resources in South Carolina.

Conclusion

SC CIC continues to evolve, leveraging partnerships and innovative solutions to address the shifting cybersecurity challenges in South Carolina. This year's highlights include the refinement and delivery of readiness exercises to a wider SC CIC audience, developing a new AI-themed phishing campaign template, and securing funds for major team expansion in the upcoming years. SC CIC remains committed to improving the cybersecurity posture of critical infrastructure in South Carolina and aims to uphold the unique culture that has been built through each member's dedication to the mission as it welcomes new voices to the table.

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”.

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

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.

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.

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.

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 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 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.

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

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.

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 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 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.

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

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.

VPN: “Virtual Private Network”; 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.