South Carolina Critical Infrastructure Cybersecurity (SC CIC)
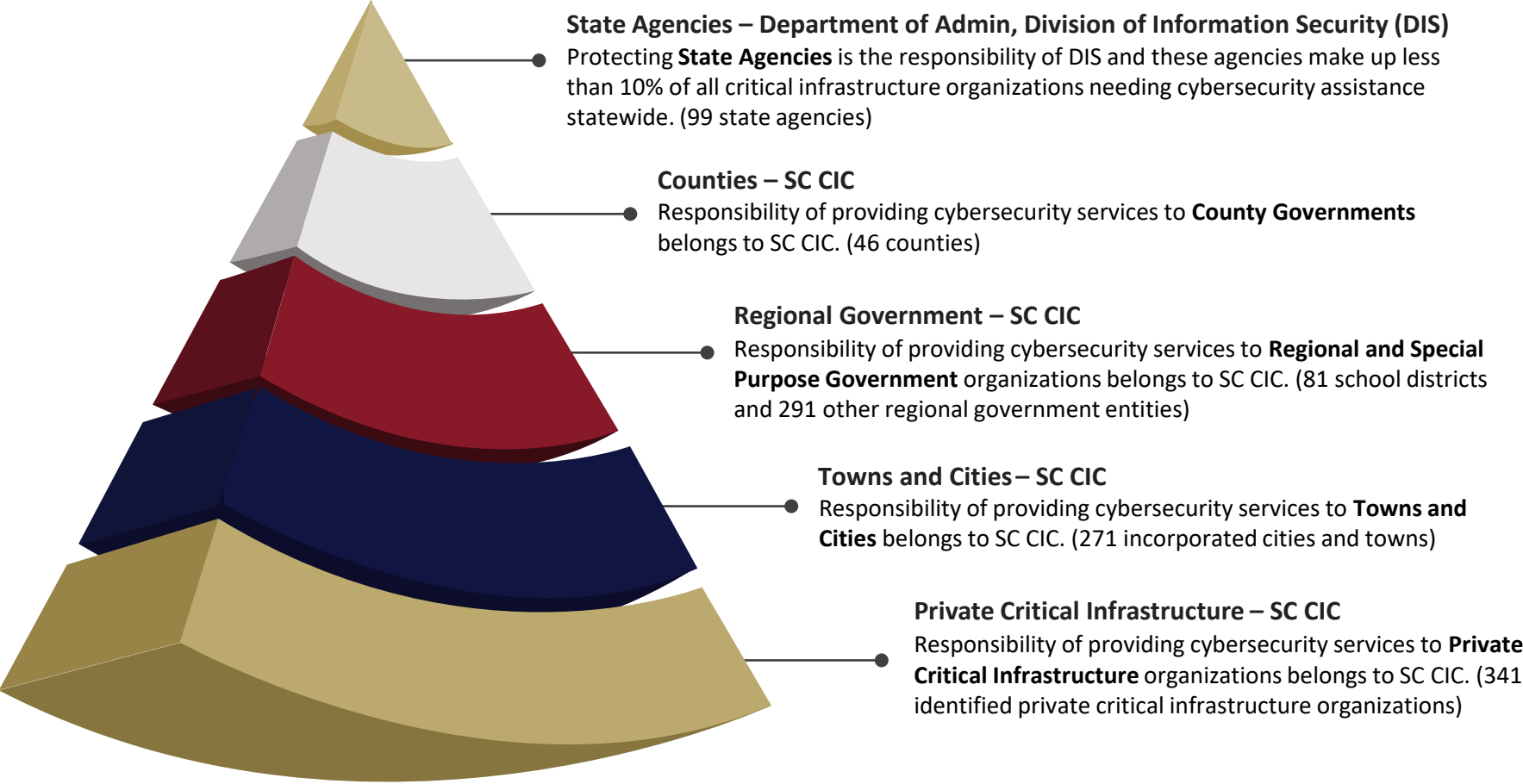
Ryan Truskey – SC CIC Director and SLED CIO

SC CIC's Role in the State
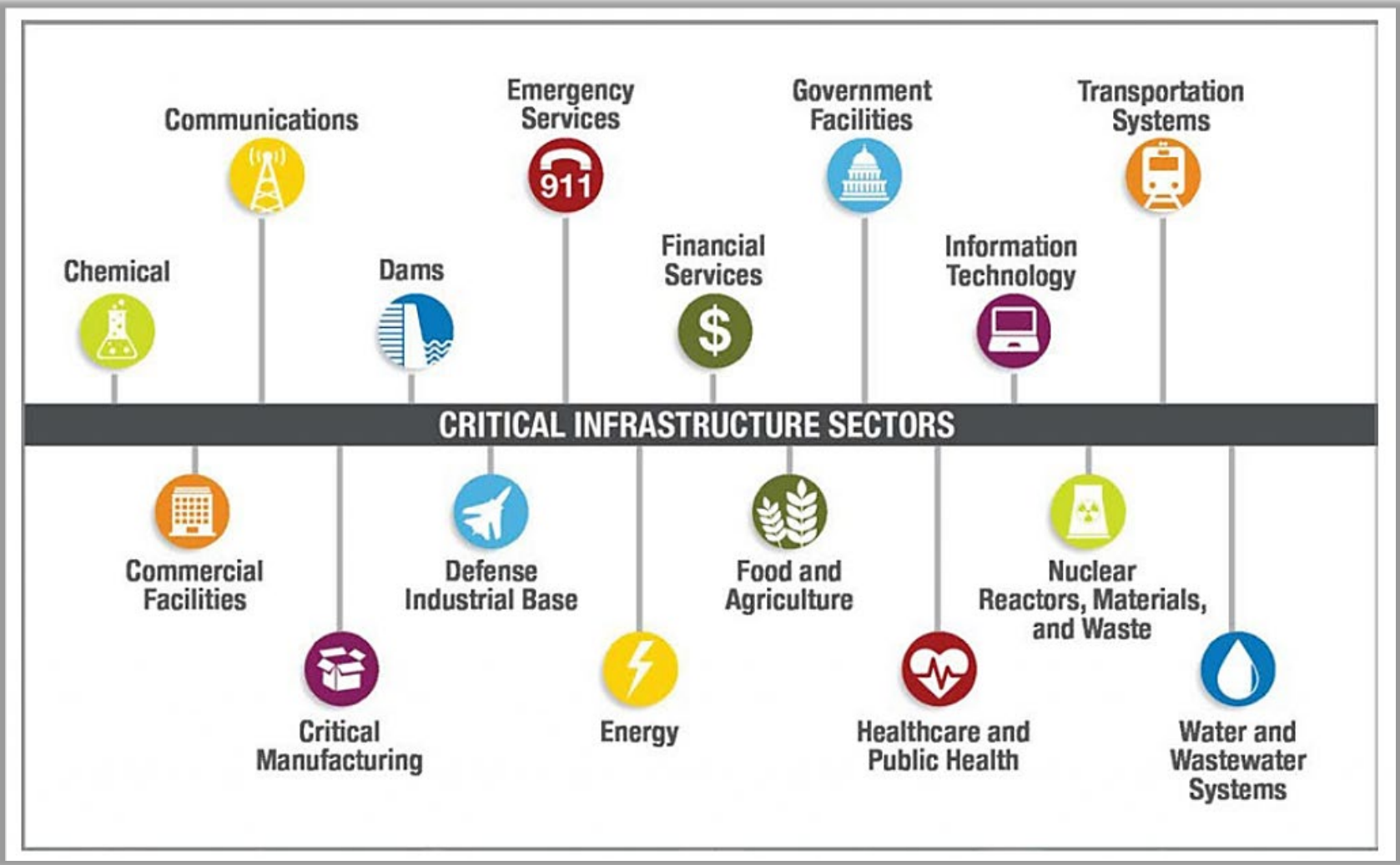
Distribution of Services

State Agencies – Department of Admin, Division of Information Security (DIS)
Protecting **State Agencies** is the responsibility of DIS and these agencies make up less than 10% of all critical infrastructure organizations needing cybersecurity assistance statewide. (99 state agencies)

Counties – SC CIC
Responsibility of providing cybersecurity services to **County Governments** belongs to SC CIC. (46 counties)

Regional Government – SC CIC
Responsibility of providing cybersecurity services to **Regional and Special Purpose Government** organizations belongs to SC CIC. (81 school districts and 291 other regional government entities)

Towns and Cities– SC CIC
Responsibility of providing cybersecurity services to **Towns and Cities** belongs to SC CIC. (271 incorporated cities and towns)

Private Critical Infrastructure – SC CIC
Responsibility of providing cybersecurity services to **Private Critical Infrastructure** organizations belongs to SC CIC. (341 identified private critical infrastructure organizations)

DIS
9%

SC CIC
91%

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

SC CIC and Critical Infrastructure

South Carolina Critical Infrastructure Cybersecurity

SC CIC Task Force

SC Law Enforcement Division
Oversees the SC CIC Program

SC Department of Administration
Division of Information Security

SC National Guard
125th Cyber Protection Battalion

US Department of Homeland Security
Cybersecurity & Infrastructure Security Agency

US Secret Service
Cyber Fraud Task Force

US Department of Homeland Security
Office of Intelligence and Analysis

SC Emergency Management Division
Cyber Incident Consequence Management

Federal Bureau of Investigations
Cyber Squad

SC Election Commission
Election and Voter Information Security

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

SC CIC in Cyber Ecosystem Study

S. CAROLINA

SC's posture and readiness is a tale of two halves, with clear strengths in protecting state assets and critical infrastructure being unmet by similar resources for assisting the general public and broader industry. The South Carolina Critical Infrastructure Cybersecurity (SC CIC) Program, in association with the SC Law Enforcement Division (SLED), has developed robust capabilities for information sharing and protection—including the development of a rapidly growing Cyber Liaison Officer program—to support the state's CI sector. Partnering with them is the SC National Guard, whose 125th Cyber Battalion (one of only five such units in the Army National Guard) provides re-

SC CIC has achieved a desirable level of coordination and centralization for the state's critical infrastructure. The survey itself enabled a strong demonstration of SC CIC's Cyber Liaison Officer (CLO) program, through which participating organizations (e.g., utilities, county and municipal government offices, healthcare institutions) may appoint a representative to serve as their official link to SC CIC. This CLO then becomes the conduit for the organization to benefit from the SC CIC network by participating in recurring information sharing sessions (e.g., on best practices and threat briefings); gaining access to technical cybersecurity services; and receiving guidance and support for assessing and improving its cybersecurity posture. During

SOUTH CAROLINA CYBERSECURITY ECOSYSTEM STUDY
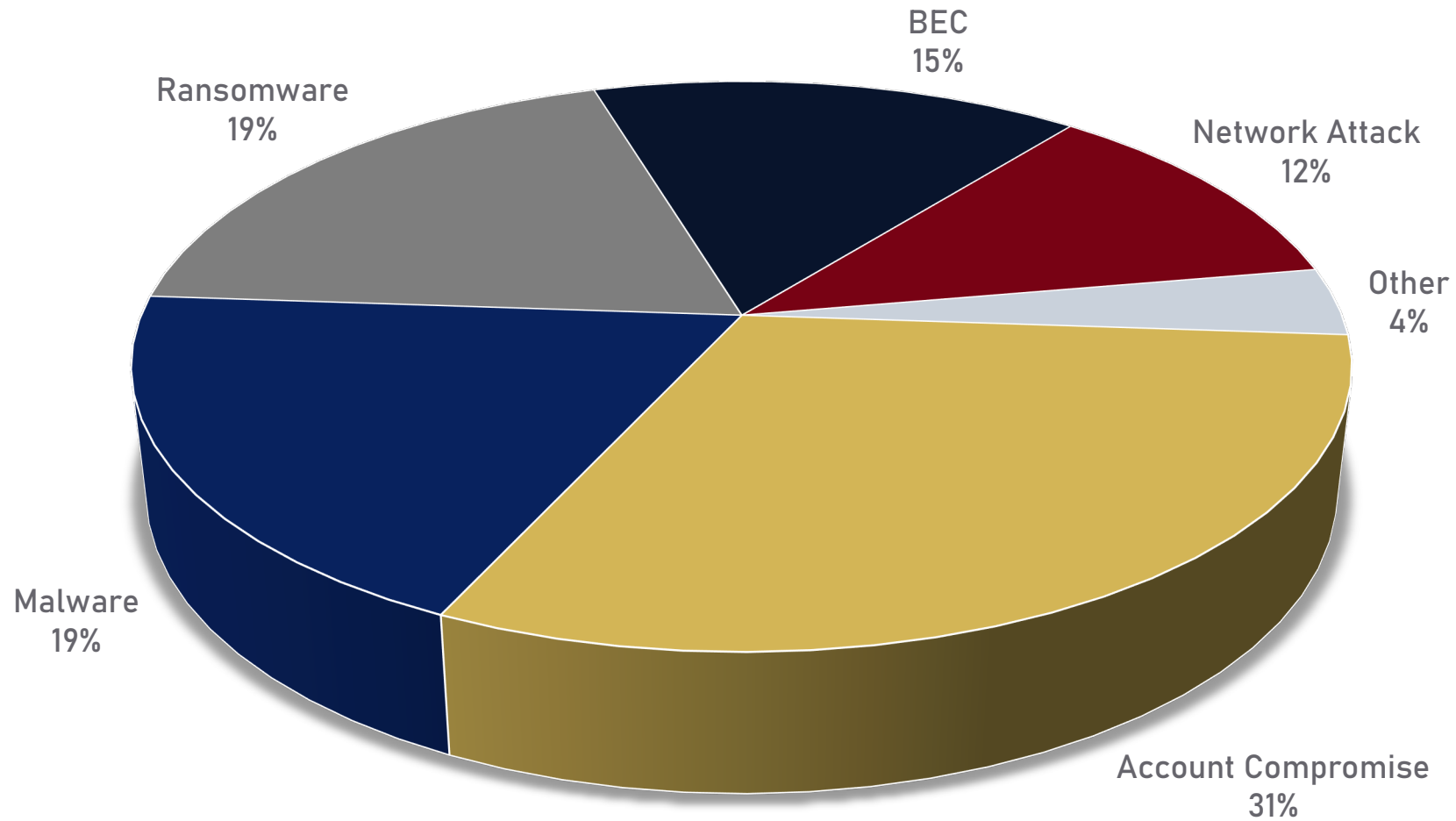
SC CIC in Cyber Ecosystem Study

IF YOU WERE ATTEMPTING TO ADVANCE A CYBERSECURITY-RELATED INITIATIVE, WHICH INDIVIDUALS WOULD YOU SEEK TO ENGAGE FOR ASSISTANCE? LIST UP TO 5.
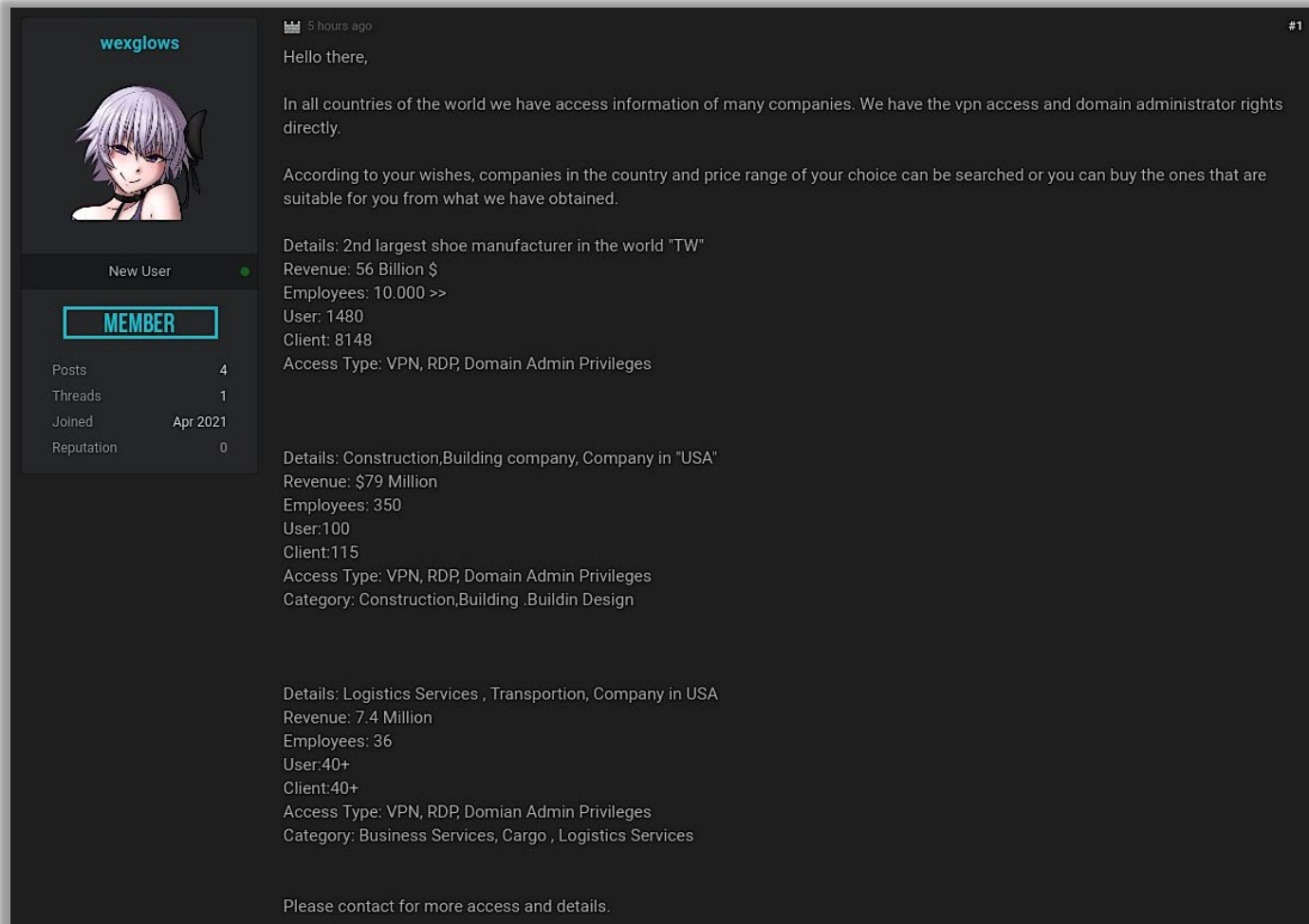
(BASED ON RESPONSES RECEIVED, WE HAVE COMBINED INDIVIDUAL REFERENCES INTO THEIR RESPECTIVE ORGANIZATIONAL AFFILIATIONS WHERE APPROPRIATE; THE LIST SHOWN INCLUDES ALL INDIVIDUALS AND ORGANIZATIONS THAT RECEIVED THREE OR MORE MENTIONS)

MENTIONS	INDIVIDUAL / ORGANIZATION
27	SC CIC / SLED
6	THE CITADEL
5	GOVERNOR McMASTER
4	UofSC SYSTEM
4	SC COMPETES
3	CLEMSON UNIVERSITY
3	SC COMMERCE
3	SC ADMIN
3	NIWC

Types of incidents in SC in 2023

South Carolina Critical Infrastructure Cybersecurity

Cyber crime: Account compromise

wexglows

New User

MEMBER

Posts	4
Threads	1
Joined	Apr 2021
Reputation	0

5 hours ago   #1

Hello there,

In all countries of the world we have access information of many companies. We have the vpn access and domain administrator rights directly.

According to your wishes, companies in the country and price range of your choice can be searched or you can buy the ones that are suitable for you from what we have obtained.

Details: 2nd largest shoe manufacturer in the world "TW"
Revenue: 56 Billion $
Employees: 10.000 >>
User: 1480
Client: 8148
Access Type: VPN, RDP, Domain Admin Privileges

Details: Construction,Building company, Company in "USA"
Revenue: $79 Million
Employees: 350
User:100
Client:115
Access Type: VPN, RDP, Domain Admin Privileges
Category: Construction,Building .Buildin Design

Details: Logistics Services , Transportion, Company in USA
Revenue: 7.4 Million
Employees: 36
User:40+
Client:40+
Access Type: VPN, RDP, Domian Admin Privileges
Category: Business Services, Cargo , Logistics Services

Please contact for more access and details.

Initial access brokers get into networks by using compromised credential or exploits on RDP or VPN devices

They sell access to ransomware groups or APTs

New group takes it from there, moving around victim's network, taking data, & eventually deploying encryption
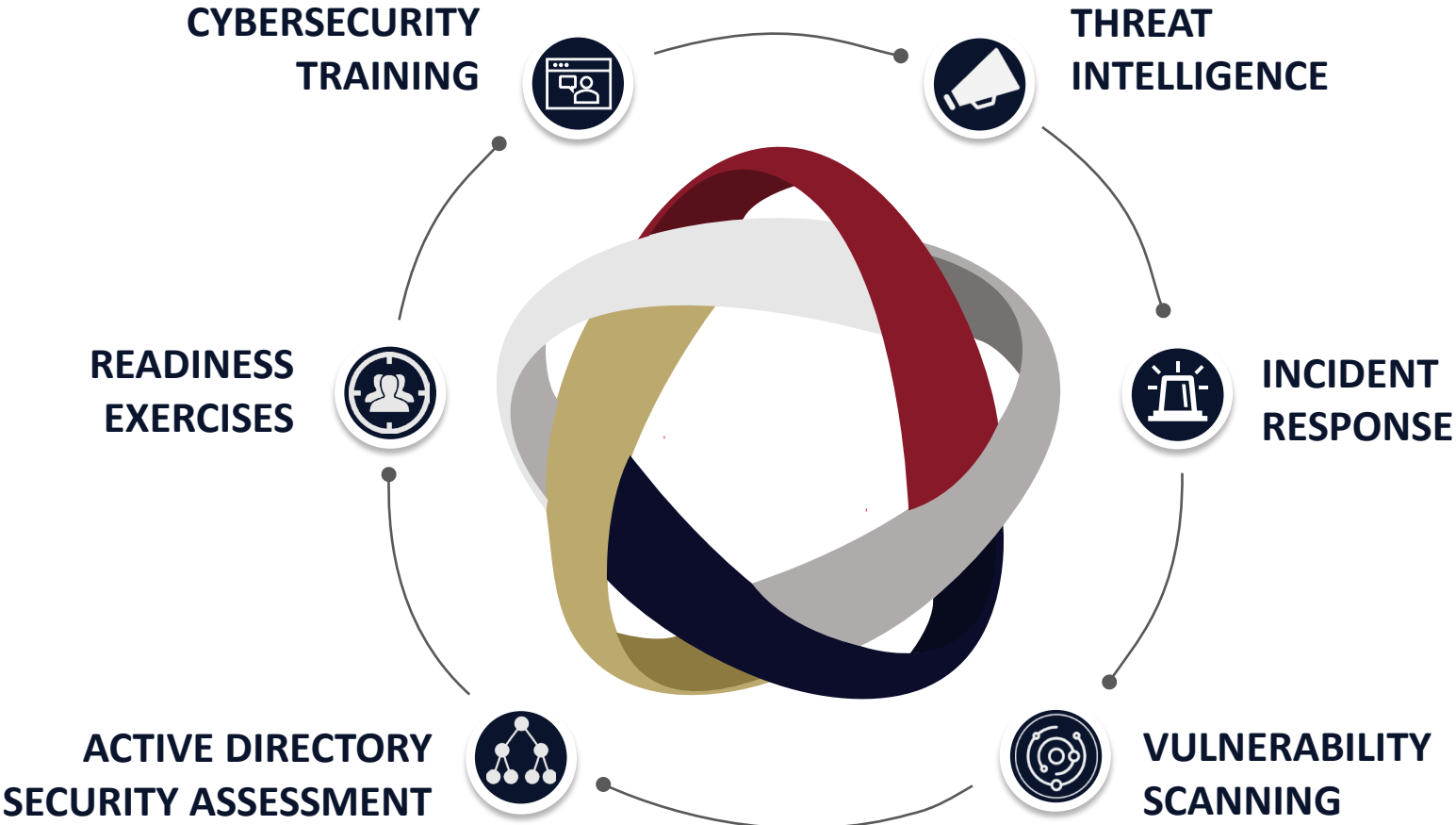
CYBER CRIME: PHISHING

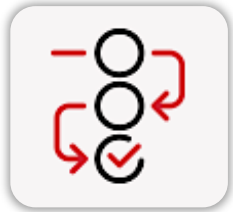Exponential Growth of an Account Compromise Phishing Attack

SC CIC Services

CYBERSECURITY TRAINING

THREAT INTELLIGENCE

READINESS EXERCISES

INCIDENT RESPONSE

ACTIVE DIRECTORY SECURITY ASSESSMENT
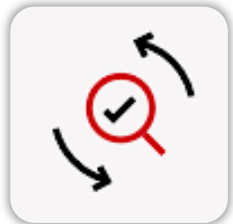
VULNERABILITY SCANNING
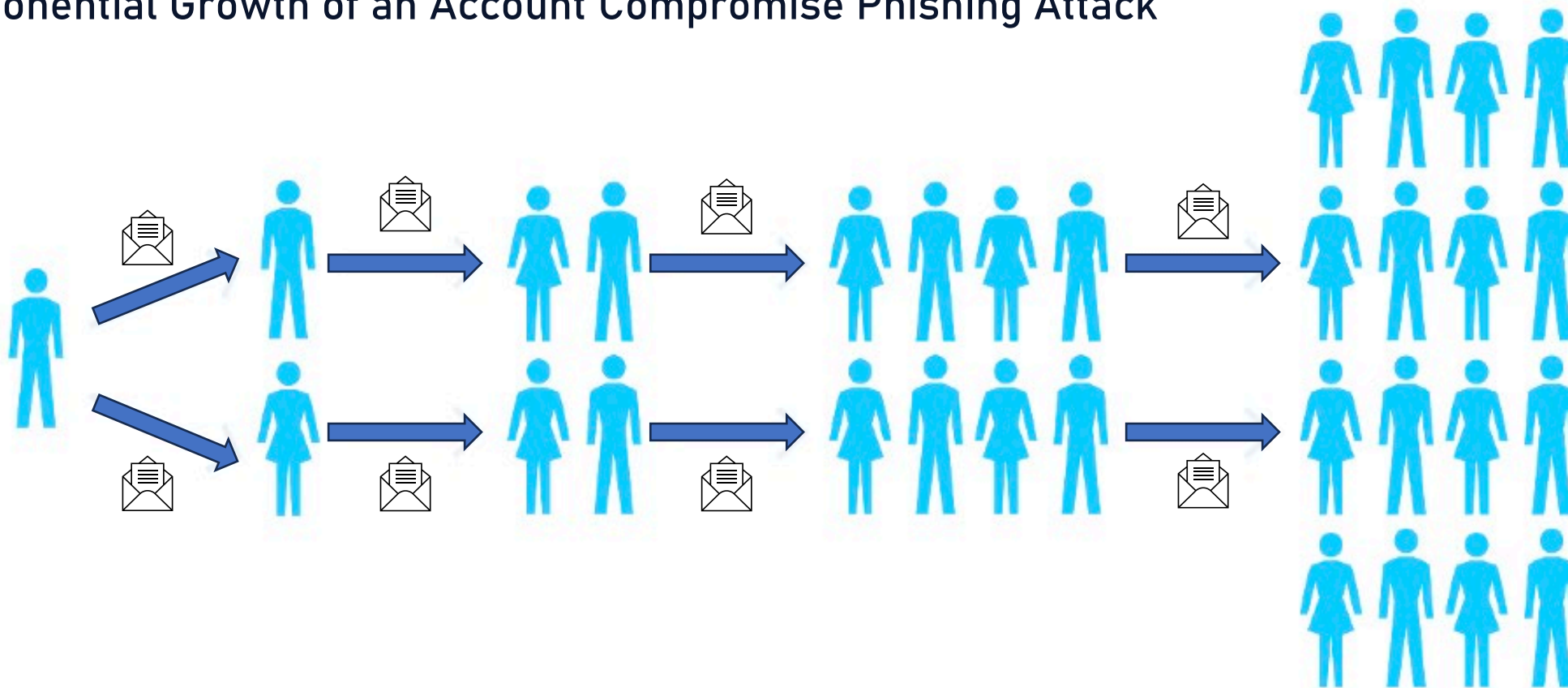
READINESS EXERCISES

Participate in tabletop exercises, training, & adversary emulation campaigns

Walk through real-world attack scenarios of current threat landscape

Re-engage to continuously improve security posture and attack readiness

READINESS EXERCISES
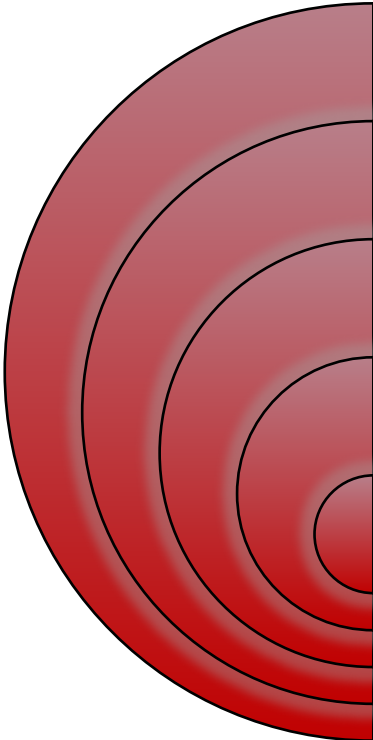
- Benefits all organizations regardless of maturity level
- Fosters interdepartmental communication
- Improves and tests incident response planning
- Helps establish and verify critical procedures
- Increases efficient use of existing security tools

CLO Monthly Call

Grants

Grants

Endpoint Detection and Response (EDR)

Cyber Range Development

SC CIC

Year 1 Projects

Threat Intelligence Services

Cybersecurity Policy Modernization Assistance

Grants

State and Local Cybersecurity Grant Program

| Funding Totals | NOFOs & Documents | Contacts |

The State and Local Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.

In 2022, the Department of Homeland Security (DHS) announced a first-of-its-kind cybersecurity grant program specifically for **State, Local, Territorial, and Tribal (SLTT) government** entities to help address cybersecurity risks and threats to information systems. This will make available **$1 billion over four years** to support approved projects.

GRANTS

Homeland Security Grant Program

Programs | Funding Totals | NOFOs & Documents

The Homeland Security Grant includes a suite of risk-based grants to assist state, local, tribal and territorial efforts in preventing, protecting against, mitigating, responding to and recovering from acts of terrorism and other threats. This grant provides grantees with the resources required for implementation of the National Preparedness System and working toward the National Preparedness Goal of a secure and resilient nation.

State Homeland Security Program (SHSP)

This program provides funding to support the implementation of risk-driven, capabilities-based State Homeland Security Strategies to address capability targets.

Grants

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

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