Georgia Cyber Innovation & Training Center

Georgia Cyber Resiliency Center – Rural Hospital Subscription Overview

AUGUSTA UNIVERSITY

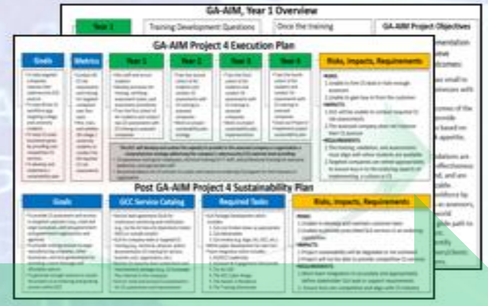
Georgia Cyber Resiliency Center

"We are committed to building the most comprehensive, affordable, and efficient cybersecurity program in Georgia and beyond, delivering world-class cybersecurity services while developing a CS workforce pipeline focusing on experiential learning, giving students real-world, marketable skills. Our program will create a direct pathway from graduation to full-time employment, improving the lives of Georgia residents while delivering exceptional value.“ – Dr. John McLain, DIT, CISSP | Director, Georgia CRC

National Cybersecurity Campaign Plan

PHASE 1

Sustainability and Regional
CS Campaign Plan Development

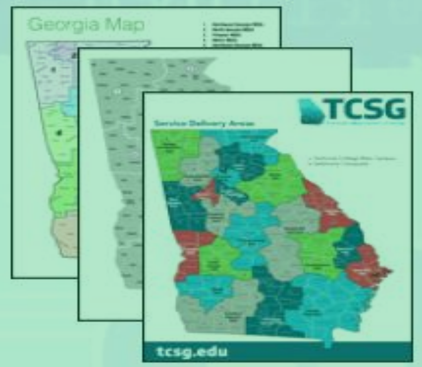


➢Utilizing the GA-AIM grant as a vehicle to:

- Develop and set the conditions to implement a post-Georgia-AIM project sustainability plan.
- Create the framework and model for a state and national CS Campaign plan to serve the CS needs of every business and industry, public and private sector vertical, by developing Cyber Resiliency Centers (CRCs)

PHASE 2

Implement Regional CS Campaign – Regional Cyber Resiliency Center (CRC) Development

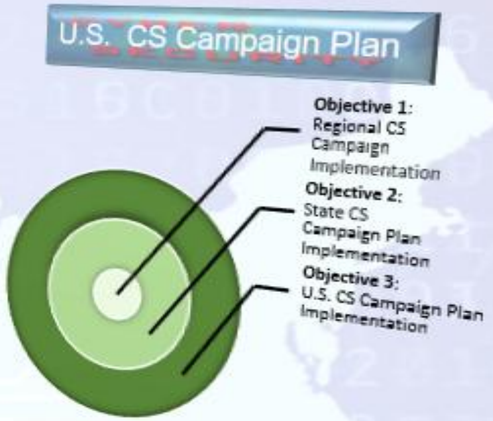


➢The Phased assessment approaches implemented for the Georgia-AIM project are utilized as the foundation for:

- Strategically targeting and implementing one or more CRC partnering with prescribed service sectors (public and private) in Georgia.
- Set the conditions to implement Phase 3 of the Campaign Plan.

PHASE 3

Implement the U.S. CS Campaign Plan

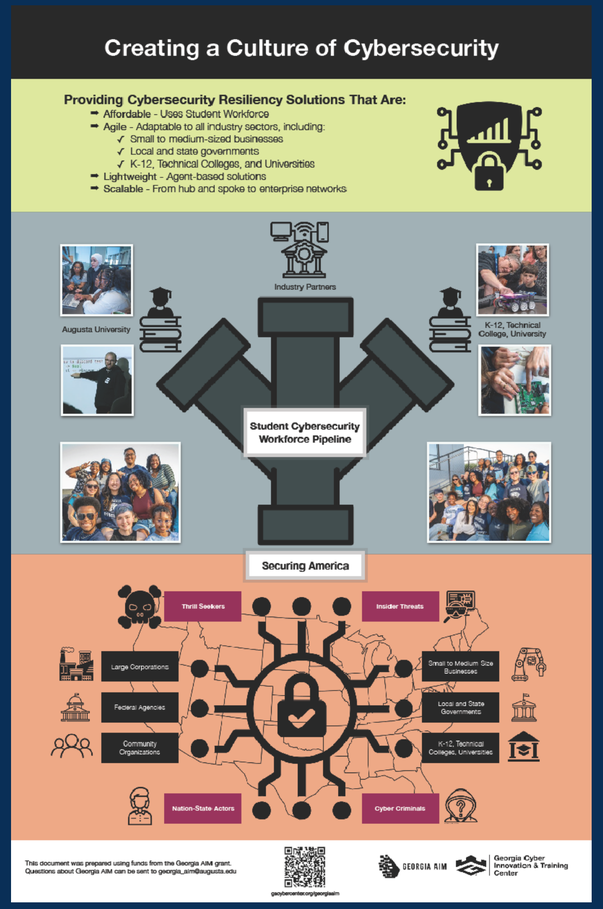


➢The primary goals of the National CS Campaign Plan are to:

- Develop secure and resilient infrastructures (business, academia, and government) for the American people.
- Goals include Cyber Defense, Risk Reduction and Resilience, Operational Collaboration, and Unification amongst all sectors – business, academia, and government (state and federal)
- Operationalize CS training, providing innovative, immersive learning experiences.
- Develop a robust and mature National CS Culture.

Revolutionizing Cybersecurity Operations

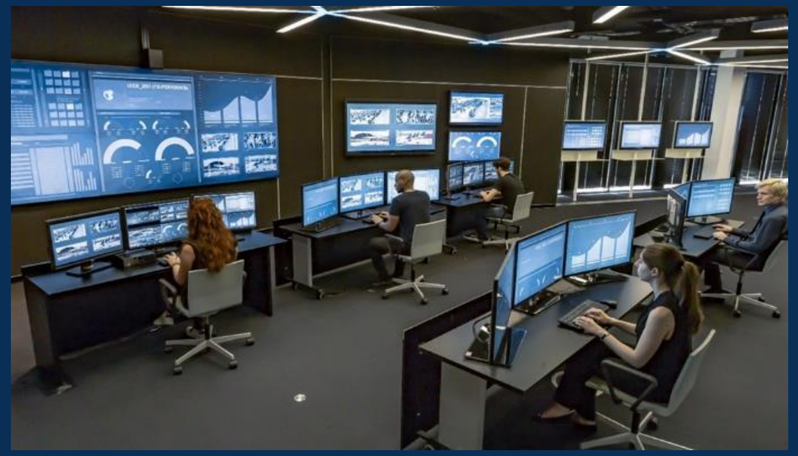
Idea



Pilot

Future State

Regional Cyber Resiliency Center



- **Assessments / Training**
- **Information Sharing**
- **CISO-as-a-Service**
- **SOC-as-a-Service**

Georgia CRC - Onboarding Process

STEP 01	SAV/Discovery – Subscription Tailoring Process
STEP 02	Implementation Strategy Development and Sign Off from the Hospital
STEP 03	Technical Onboarding (APIs, Sensors, Scans, all logs)
STEP 04	Tuning and Hand-Off to Production – Technical and Compliance Teams

Cybersecurity Subscription Plan Phases

Phase 1

- SAV*
  - Assess
  - Monitor
  - Harden
- Compliance

* SAV = Site Assistance Visit

Phase 2

- CS** Culture Improvement
  - CS Training
  - Compliance

** CS = Cybersecurity

Phase 3

- CS Sustainment
- Pen-Testing
- Continuous Online Compliance
- Annual Cyber Exercise

Sample: Tailored Subscription Service Offerings

- Virtual CISO-as-a Service
- Cybersecurity Risk Assessment
  - ✓ Technical scan of the network
  - ✓ Executive Summary Brief
  - ✓ Tabletop Exercise
  - ✓ Policy and SOP development
- Cybersecurity (CS) Training
  - ✓ Initial/annual CS awareness training
  - ✓ Interactive assessments / Quizzes
  - ✓ Three industry CS certifications – training and voucher per hospital per year
- Cyber Pathfinder (organizational access) Cyber workforce development tool
  - ✓ National Initiative for CS Education (NICE) framework aligned
- Health Care Cyber Sentinel (Start FY 2027)
  - ✓ World-class cyber exercise that is scenario-driven
  - ✓ Validate hospital detection and response in a safe environment
  - ✓ Conducted annually
- Annual Pen Testing – Red Team as-a-Service (RTaaS) (Start FY 2027)
  - ✓ Red Team Site Assessment Visit (RT-SAV)
  - ✓ Rapid Scan – Baseline
- HITRUST compliance framework
- CrowdStrike EDR solution

Subscription Service Offerings – Currently 25

- Virtual CISO-as-a Service
- Cybersecurity Risk Assessment
- Cybersecurity (CS) Awareness Training
- 3 – Industry CS Certifications – Training and Test Vouchers
- Cyber Pathfinder (organizational access)
- RMM Capability
- SOC Monitoring Services
- Tier Level Triage
- Weekly and Monthly Compliance Reports
- Compliance Policy Development
- Acceptable Use Policy
- System Security Plan Development
- Federal Continuity of Operations Development
- Non-Federal Continuity of Operations Development
- Health Care Cyber Sentinel (Start FY 2027)
- Annual Pen Testing – Red Team as-a-Service (RTaaS) (Start FY 2027)
- HITRUST compliance framework
- CrowdStrike EDR solution
- Network Mapping
- Leadership Training – Executive Summary and Tabletop Exercise Development
- CMMC Level 1 Preparation
- CMMC Level 2 Preparation
- SOC Level 2 Preparation
- 3-5 Year Strategic Planning
- Knowledge Management Development

EDR – CrowdStrike Falcon Complete and HITRUST e1, i1, and r2 compliance

- CrowdStrike Falcon Complete
  - World-class EDR solution
  - No cost to rural hospitals – through the CMS funded program
  - Sustainability

- HITRUST Compliance
  - World-class compliance framework
  - No cost to rural hospitals

Backup Slides

Georgia CRC - Judy SIEM and Internship Program Partnership

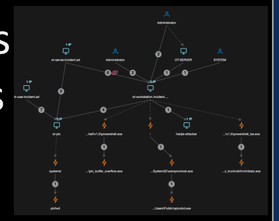
MSSP Alert
A CRA Resource

Top 250 MSSPs
2024 EDITION

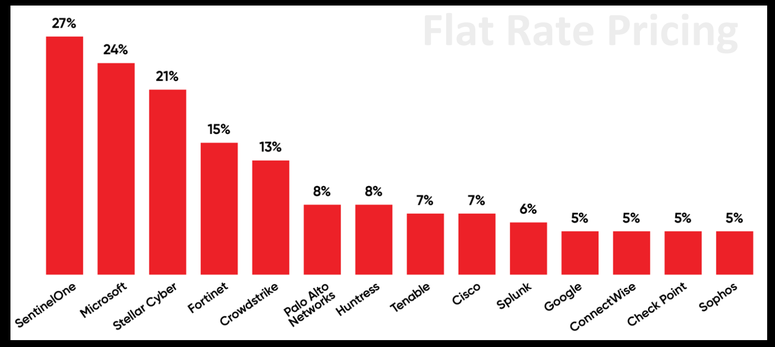
22 Judy Security

Open XDR is Tool Agnostic

Leverage Existing Cyber Tools
3500 Parsers and Connectors
Immersive Experience
Latest AI Technologies
MITRE Kill Chain



No other MSSP offers Affordable



Proven Program

15-20 Hours/Week
$15/hour
Mentorship Program
SOC Leveraging Latest AI
Letter of Recommendation
300+ placements in 3 years

UNIVERSITY OF MICHIGAN

E

Judy Security - Referral from Pilot Project

‘Presented as a solutions provider by the AU CRC Team, Judy Security introduced us to a SIEM solution using the Steller Cyber framework. Within days we had functional communications between our critical infrastructure components and Stellar Cyber. Judy Security both walked us through the setup process and performed the setup where their expertise was beyond ours. We now have a fully operational SIEM with a 24x7 SOC to give us the peace of mind that we (with Judy Security’s help) are effectively monitoring and protecting our technical environment.’

Norman P. Ludecke

I.T. Director, HIPAA Security Officer

Memorial Hospital & Manor

The Rise of Agentic AI

Open XDR State of the Art Predictive AI

SaaS Offering

Virtual

On-Prem

Normalization

Network

Endpoint

SaaS

Cloud

Vulnerability

Identity

NORMALIZATION

ENRICHMENT

ML-Based Alerts

Rules-Based Alerts

3rd Party Alerts

Blue Team for Security Operation

Triage Alerts

Creates & Prioritizes Cases

Detects & Investigates Raw Data

Gather External Context On-Demand

Summarizes & Acts

Model Improves Automatically

Human Analysts

Validate, assist, and teach the AI.

Judy Security - Concierge Installs

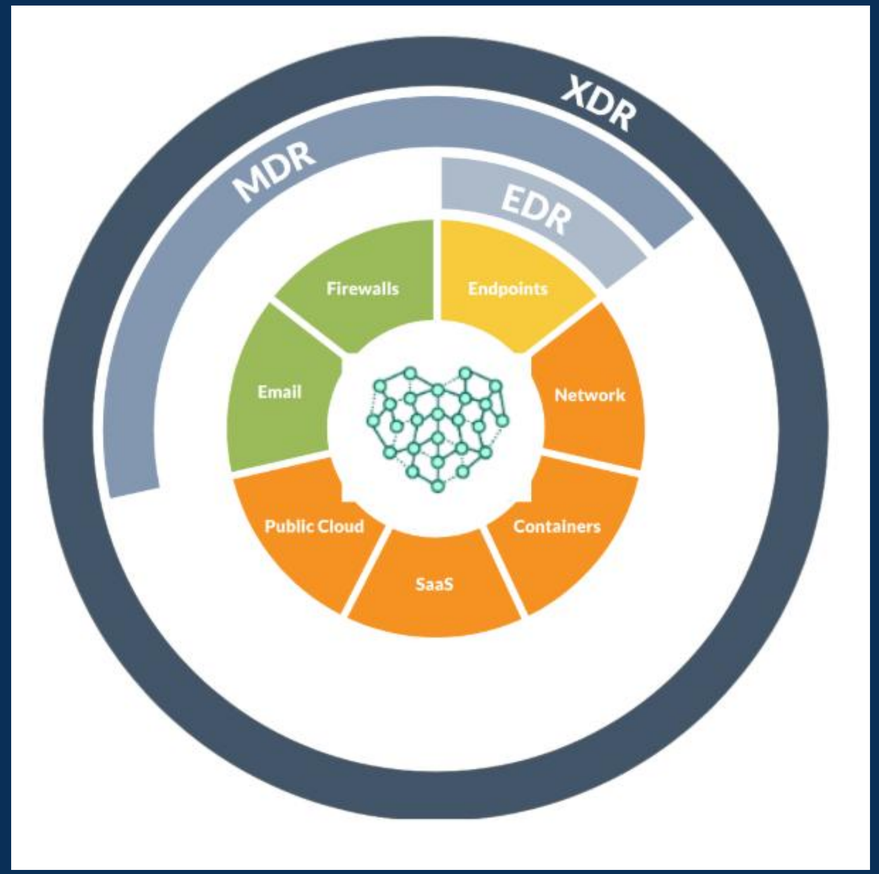
Organizations are ALWAYS very busy
Installs can take time

- Collecting passwords and account info
- Setting up sensors
- Testing the connections to make sure logs are being ingested

We have the solution!!!

1. Provide temporary admin access for the API integrations to the SOC team
2. Provide virtual sensor servers with a login
3. We will do the implementation
4. Remove the admin access and you are done!

Best part - FREE OF CHARGE!!!



Judy Security